КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2019.4.613
УДК 004.056

Хлапонін Юрій Іванович
доктор технічних наук, професор
Київський національний університет будівництва і архітектури, м. Київ, Україна
OrcID: 0000-0002-9287-0817
y.khlaponin@gmail.com

Кондакова Світлана Віталіївна
кандидат фізико-математичних наук, доцент
Київський національний університет будівництва і архітектури, м. Київ, Україна
OrcID: 0000-0003-0626-6849
s_kondakova@ukr.net

Шабала Євгенія Євгенівна
кандидат технічних наук, доцент
Київський національний університет будівництва і архітектури, м. Київ, Україна
OrcID: 0000-0002-0428-9273
wild_miledi@ukr.net

Юрчук Лілія Петрівна
студент
Київський національний університет будівництва і архітектури, м. Київ, Україна
OrcID: 0000-0002-4421-3476
lili.yurchyk@gmail.com

Демянчук Павло Сергійович
студент
Київський національний університет будівництва і архітектури, м. Київ, Україна
OrcID: 0000-0001-5140-9672
demianchuk.pasha2@gmail.com

АНАЛІЗ СТАНУ КІБЕРБЕЗПЕКИ В ПРОВІДНИХ КРАЇНАХ СВІТУ

Анотація. Стаття присвячена дослідженню тенденцій кіберзлочинності, що є загрозою інформаційній безпеці країни. Визначено місце та роль кібербезпеки в системі національної безпеки. Було проаналізовано стан системи захисту від кібератак в розвинених країнах світу, таких як Франція, Японія, Китай, Південна Корея та Велика Британія. Виявлені основні недоліки та перспективи забезпечення захисту кіберпростору. Використання сучасних інформаційних технологій у державних структурах, а також у суспільстві в цілому, висуває вирішення проблем інформаційної безпеки в число основних. Економіка, логістика та безпека країни все більше залежать від технічної інфраструктури та її захищеності. Для підвищення ефективності боротьби з кіберзлочинністю, розвинені країни світу досить давно почали відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Інциденти в сфері кібербезпеки позначаються на життєдіяльності споживачів інформаційних і багатьох інших послуг та кібератаки, націлені на різноманітні об'єкти інфраструктури систем електронних комунікацій чи управління технологічними процесами. Сучасні світові тенденції поширення кіберзлочинності та посилення кібератак свідчать про зростання значення боротьби з нею для подальшого розвитку суспільства, що у свою чергу зумовлює віднесення певних груп суспільних відносин кіберсфери до компетенції правового регулювання. Ситуація, яка склалася на сьогоднішній день з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами, розробки інформаційних систем та методів, спрямованих на забезпечення кібербезпеки країни. Необхідними задачами є розробка національної стратегії з кібербезпеки, котра міститиме тактичні та стратегічні пріоритети і завдання у даній сфері для державних органів. Отже, питання безпеки кіберпростору, боротьби з кіберзлочинністю є актуальним як на міжнародному рівні, так і на рівні окремої країни, а тому потребує подальшого розгляду.

Ключові слова: кіберпростір; кібератаки; захист; кібербезпека; безпека держави.

ISSN 2663 - 4023

1. ВСТУП

Кіберпростір став невід'ємною частиною життя будь-якої сучасної нації. Це сприяє вирішенню соціальних проблем і має великий потенціал з точки зору економічного зростання та інноваційної діяльності, світове співтовариство вважає його стимулом для розвитку, який надає можливості для здійснення комунікацій та реалізації суспільних відносин.

З огляду на це, кібератаки на інформаційну інфраструктуру стали реальною загрозою і є однією з пріоритетних проблем національної безпеки та управління ризиками.

Постановка проблеми. Нові руйнівні практики розвиваються в кіберпросторі, включаючи злочинне використання Інтернету (кіберзлочинність), шпигунство з політичними або економічними цілями, а також напади на критичну інфраструктуру (транспорт, енергетика, зв'язок тощо) з метою саботажу. Виходячи з урядових чи неурядових гравців, ці кібернапади:

• не обмежуються кордонами або відстанню;

• є анонімними, і дуже важко дійсно визначити справжнього винуватця, який часто діє під прикриттям бот-мереж або посередників (проксі);

• можуть здійснюватися з відносною легкістю, з невеликими витратами або ризиком для зловмисника.

Вони мають на меті поставити під загрозу безперебійне функціонування інформаційних та комунікаційних систем (ІКС), що використовуються громадянами, підприємствами та адміністраціями, і навіть фізичну цілісність інфраструктури, що має вирішальне значення для національної безпеки.

Кібербезпека охоплює всі заходи безпеки, які можуть бути вжиті для захисту від цих нападів. Значне зростання складності та інтенсивності кібератак в останні роки змусило більшість розвинених країн посилити свій захист і прийняти національні стратегії кібербезпеки. Тому актуальною є проблема забезпечення захисту кіберпростору в світі.

Аналіз останніх досліджень і публікацій. В статтях [1-4] були висвітлені проблеми, які існують в системах захисту захисту кіберпростору Китаю та основні задачі, які ставить перед собою ця країна. В статтях [5-8] визначені напрямки захисту від кіберзагроз, захисту кіберпростору та національної безпеки в країнах ЄС, зокрема Франції та Великої Британії.

Метою статті є висвітлення стану забезпечення захисту кіберпростору в розвинених країнах світу, що дасть змогу проаналізувати проблеми та перспективи розвитку системи захисту кіберпростору.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Національний кібербезпековий арсенал Франції. Стратегічні позиції, прийняті в останні роки на найвищому політичному рівні, закріпили місце кібербезпеки як пріоритет роботи уряду. Франція провела глибокий перегляд своєї політики оборони та національної безпеки у 2008 та 2013 роках, а нові пріоритети були визначені та затверджені тодішнім Президентом Французької Республіки. До них відносяться запобігання та реагування на кібератаки, які були визначені як головний пріоритет в організації національної безпеки.

ISSN 2663 - 4023

У липні 2009 року було створено Французьке агентство мережевої та інформаційної безпеки (ANSSI, Національна агенція з питань інформаційної безпеки) для вирішення все більшого виклику кібератак, відповідно до рекомендацій Білої книги з питань оборони та національної безпеки - це міжміністерське агентство, приєднане до кабінету прем'єр-міністра. Значення ANSSI було піднято на початку 2011 року, коли Агентство стало національним органом захисту інформаційних систем.

Після створення Агентства Франція опублікувала національну стратегію оборони та безпеки інформаційних систем у 2011 році. Біла книга 2013 року підтвердила кіберзагрозу і конкретно визначила загрозу саботажу проти критичної інфраструктури.

В Європейському Союзі стратегія кібербезпеки була презентована у лютому 2013 року Європейською Комісією та Європейською службою зовнішньої діяльності (EEAS). Франція активно сприяє впровадженню п'яти основних напрямків:

- загальна стійкість ЄС (включаючи органи ЄС);
- боротьба з кіберзлочинністю;
- питання кіберзахисту в рамках Спільної політики безпеки і оборони;
- промислові питання;
- міжнародна політика у сфері кіберпростору.

В країнах НАТО кіберзахист є основним аспектом оновлення Альянсу та його адаптації до нових загроз. Після прийняття нової стратегічної концепції під час Лісабонського саміту в листопаді 2010 року, 28 червня 2011 року було затверджено політику НАТО щодо кіберзахисту, а у вересні 2014 року «розширено» під час саміту у Ньюпорті (Уельс).

В умовах швидкого розвитку інтернету та концепції IoT (Internet of Things), атаки стаюсь все більш віртуозними та складними у передбаченні та протидії. То ж Франція приділяє багато уваги, сил та коштів, щоб перейняти світовий досвід та застосувати його у себе вдома, таким чином створивши одну з найбільш вдалих систем протидії кіберзлочинності. Важливо зазначити, що така серйозна система та такі суттєві заходи безпеки не обмежують основних прав громадян, організацій та ЗМІ. Хоч і не існує зараз досконалої системи захисту від усіх можливих кіберзагроз, Франція впевнено розбудовує власний захист кіберпростору, що дозволяє їй без зайвих загроз проводити внутрішню та зовнішню політику та утримувати провідні позиції у вирішенні світових викликів.

Стан кібербезпеки в Японії. Японія є країною, яка позиціонує себе однією з найбільш розвинених інформаційних країн у світі і для того, щоб зберегти свою репутацію, вона повинна забезпечити гідний рівень кібербезпеки. Діапазон груп, які постраждали від кібератак (від фізичних осіб та окремих сімей до складних підприємств соціальної інфраструктури) швидко розширюється. Незважаючи на всі зусилля японського уряду, ризик інформаційної атаки збільшується. Цей ризик впливає на такі сфери, як національна безпека, управління ризиками та конкурентоспроможність японської економіки.

Японська промисловість відстає від своїх американських та європейських аналогів щодо оцінки кіберзагроз. Згідно з державною статистикою лише 55 відсотків японських компаній проводять оцінки ризиків кібербезпеки, порівняно з приблизно 80 відсотками в США і 65 відсотків у Європі.

10 червня 2013 року Рада з політики інформаційної безпеки Японії прийняла Стратегію кібербезпеки. Японський уряд раніше використовував формулювання «інформаційна безпека» для своєї політики і основоположних планів. Однак у зв'язку зі зростаючим числом кіберзагроз, які виходять за рамки інформаційної безпеки, таких, наприклад, як диверсія щодо об'єктів життєзабезпечення населення, в Токіо було

ISSN 2663 - 4023

прийнято рішення використовувати термін «кібербезпека» для того, щоб вперше розглянути всі ці проблеми.

Стратегія спрямована на розвиток «провідного в світі», «сталого» і «динамічного» кіберпростору і перетворення Японії у світового лідера в області кібербезпеки. Для реалізації цих цілей в документі передбачені чотири основні принципи:

забезпечення вільного обміну інформацією;

забезпечення нових заходів у відповідь на те, що ризики стають більш серйозними;

прийняття адекватних заходів щодо кіберзагроз на підставі оцінки ризиків;

вжиття заходів і взаємодія з іншими державами на підставі їх власної соціальної відповідальності.

Державним органом, що регулює взаємовідносини в галузі кібербезпеки є Національний центр інформаційної безпеки (NISC), який розробляє проекти урядових стандартів щодо заходів з інформаційної безпеки, формулює рекомендації на основі результатів оцінки стану кібербезпеки та сприяє впровадженню заходів щодо покращення стану кібербезпеки.

Китай. Китай є вразливим, бо не має єдиної об'єднаної стратегії. Основні завдання в сфері кіберзахисту, які ставить перед собою Китай:

1. Захист суверенітету кіберпростору
2. Захист критичної інформаційної інфраструктури (ICI)
3. Створення здорової онлайн-культури
4. Боротьба з кіберзлочинністю, шпигунством і тероризмом
5. Поліпшення кібер-управління
6. Підвищення базової кібербезпеки
7. Підвищення можливості захисту кіберпростору
8. Зміцнення міжнародного співробітництва

Протягом наступних одного-двох років Китай продовжуватиме здійснювати контроль над інформацією та технологіями через CSL та пов'язані з ними положення. Локалізація даних, особливо для "важливих" даних, буде потрібна для всіх компаній, що працюють в Китаї. Регулятори також зобов'язуються використовувати технологію, яка відповідає їхнім вимогам, щоб бути «безпечними та керованими» (наприклад, шифрування).

Заходи правозастосування здебільшого продовжуватимуть зосереджуватись на системах та інформації, що знаходяться у розпорядженні китайських урядових установ та державних і приватних підприємств, які ставляться до таких кіберзагроз цілком серйозно, про що свідчать ухвалені ними нормативні документи, що регулюють політику із захисту власного кіберпростору та основних напрямів протидії діяльності ворожих груп.

Південна Корея. Частота і серйозність кібератак спонукали уряд Південної Кореї переоцінити свою стратегію кібербезпеки. Є три установи, що обладнані для вирішення питань кібербезпеки: Національний центр кібербезпеки, Корейське агентство Інтернет та безпеки (KISA), а також Центр реагування на кібертерор Національного поліцейського агентства. Ці установи несуть відповідальність за виявлення, запобігання та реагування на кібератаки та загрози безпеці. Крім того, була заснована школа, що спеціалізується на кібервійнах, з наміром збільшити експертів з безпеки до 7000 до кінця 2019 року.

Перспективами в системі захисту кіберпростору у Південній Кореї є:

−Шифрування для доступу до мережі;

−Системи профілактики вторгнень (IPS);

−Розширена стійка загроза (APT);

−Хмарні обчислення;

ISSN 2663 - 4023

−Безпека IoT.

Для американських фірм існує безліч можливостей забезпечити найсучасніші рішення з кібербезпеки для критичної інфраструктури в Південній Кореї. Завдяки передовій ІКТ-інфраструктурі, Південна Корея є ідеальним ринком для американських фірм, які прагнуть перевірити рішення щодо кібербезпеки, перш ніж розгортати їх на інших ринках.

Щоб увійти на ринок кібербезпеки, Комерційна служба США в Кореї рекомендує американським технологічним фірмам співпрацювати з провідними південнокорейськими компаніями, які підтримують існуючі мережі збуту на фінансових, енергетичних та інших ключових ринках інфраструктури, і повністю знають місцеві ринкові характеристики та унікальні нормативні вимоги.

Великобританія. Загальновідомо, що Сполучене Королівство є країною, яка особливо ретельно охороняє свої секрети. Ілюстрацією цього може служити, зокрема, історія системи шифрування з відкритим ключем. Вперше її алгоритм був розроблений та опублікований у 1977 році вченими Массачусетського технологічного інституту Рональдом Райвестом, Аді Шаміром та Леонардом Адлеманом. Хоча першість в цьому питанні належить британським вченим Кліфорду Коксу та Малкольму Уільямсону, які зробили це ще у 1973 році, проте аж до 1997 року сам алгоритм та його використання був засекречений [5].

Сучасна система кіберзахисту потребує надзвичайно талановитих кадрів, які відповідна спецслужба шукає серед різних груп населення. В NCSC розроблена серйозна система підбору кадрів. Для цього всім, хто вивчає прикладні технології, математику чи мови в організації надають можливість участі у реальних проектах.

Програма CyberFirst є головною частиною Національної програми уряду. Вона охоплює широкий спектр діяльності, стипендіальні програми, літні школи, тощо. Це програма для студентів та талановитої молоді і очолює її NCSC, яка пропонує комплексний пакет фінансової допомоги та навчання навикам роботи з кіберпростором для талановитих початківців.

Детальний аналіз закритих та нині діючих програм показує, що з року в рік молодшає їх цільова аудиторія. Найбільш вражає те, що зараз деякі пропозиції стосуються молоді, яка закінчить школу в період 2020-2023 років. Проте з відмінними оцінками по предметам STEM.

Претендувати на роботу в системі GCHQ можуть, зокрема, люди з особливими потребами, проте вимоги до найближчого оточення, громадянство Сполученого Королівства та проживання на території країни більшості часу останні 10 років є беззаперечними.

«To disclose or not to disclose» - під такою промовистою назвою на сайті відомства (GCHQ та відповідного структурного підрозділу NCSC) 29 листопада 2018 року було зроблено публікацію. Як і з решти матеріалів, з неї незмінно слідує, що інтересам національної безпеки Сполученого Королівства краще служить зберігання та накопичення знань, проте не їх оприлюднення.

Є два способи боротьби з вразливостями кіберпростору. Перший – розкрити вразливість, щоб вона могла бути зафіксована та приносила користь глобальним користувачам технологій. Другий – зберегти знання про цю вразливість та використати її в майбутньому з розвідувальною метою та для порушення діяльності тих, хто прагне збитків у Сполученому Королівстві, [6]. Рішення на користь одного з цих підходів приймається колегією провідних світових експертів трьох відомств (GCHQ, NCSC та Міністерства оборони).

13 вересня 2016 році на Біллінгтонському самміті з кібербезпеки у Вашингтоні керівник NCSC К'яран Мартін наголосив «…незважаючи на те, що сучасна робота в області кіберзахисту потребує більш відкритого підходу, надзвичайно важливим залишається збереження статусу Сполученого Королівства як однієї з небагатьох суверенних криптографічних держав для її самих важливих? («most sensitive») секретів», [7].

Про високий рівень роботи Національного центру британської кібербезпеки свідчить той факт, що саме це відомство компанією Microsoft в рамках програми Microsoft Bug Bounty було відзначено у першому кварталі 2018 року як одне з 5 найбільш ефективних, отримало визнання заслуг та нагороду в 15 000 доларів [8].

В Сполученому Королівстві, як в самодостатній суверенній державі, є власні стандарти, починаючи з дорожніх знаків у милях та ярдах, молочних пляшок у пінтах, специфічної конструкції розеток і закінчуючи більш серйозними питаннями життєзабезпечення. При цьому це не робить країну менш бажаною для різного роду співробітництва. Швидше навпаки, викликає неабияку повагу та зацікавленість.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сьогодні головною темою обговорення у світі має стати зміцнення кібербезпеки та скорочення кількості кібератак в кіберпросторі. Дана проблема потребує якнайшвидшого вирішення, оскільки створені зразки кіберзброї вирізняються глобальною досяжністю, практично миттєвим впливом без будь-якого способу отримання попередження про її застосування. Кіберзахист - це єдине, що може запобігти втратам інформації та втручанню одних країн в безпеку інших. В ході аналізу стану кібербезпеки в розвинених країнах світу були визначені основні напрямки захисту від кіберзагроз, захисту суверенітету кіберпростору та національної безпеки в провідних країнах світу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1].Cybersecurity strategy (2018) [Електронний ресурс]. – Режим доступу: https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf
[2].China publishes first national cybersecurity-strategy [Електронний ресурс]. – Режим доступу: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy.
[3].Cyberspace Administration of China [Електронний ресурс]. – Режим доступу: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm
[4].China's Cyber Security Law: how prepared are you? [Електронний ресурс]. – Режим доступу: https://www.controlrisks.com/campaigns/china-business/chinas-cyber-security-law.
[5].Welcome to GCHQ.Pioneering a new kind of security for an ever more complex world [Електронний ресурс]. – Режим доступу: www.gchq.gov.uk.
[6].Equities process Publication of the UK's process for how we handle vulnerabilities. [Електронний ресурс]. – Режим доступу: www.ncsc.gov.uk/blog-post/equities-process.
[7].Tencent Xuanwu Lab Security [Електронний ресурс]. – Режим доступу: http://blogstechnet.microsoft.com/msrc/2018/04/20/recognizing-q3-top-5.
[8].A new approach for cyber security in the UK (2016) [Електронний ресурс]. – Режим доступу: https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk.
[9].Кондакова С.В. Кібербезпека в Великобританії. Перші враження [Текст] / С.В. Кондакова, Ю.І. Хлапонін // Бизнес и безопасность. – 2019. – № 1.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

Yurii I. Khlaponin
doctor of Technical Sciences, Professor, Head of the Department of Cybernetic Security and Computer Engineering
Kyiv National University of Construction and Architecture, Kyiv, Ukraine
OrcID: 0000-0002-9287-0817
yfcnz0408@ukr.net

Svitlana V. Kondakova
Ph.D., associate professor, associate professor of Department of cyber security and Computer Engineering
Kyiv National University of Construction and Architecture, Kyiv, Ukraine
OrcID: 0000-0003-0626-6849
s_kondakova@ukr.net

Yevheniia Ye. Shabala
Ph.D., associate professor, associate professor of Department of cyber security and Computer Engineering
Kyiv National University of Construction and Architecture, Kyiv, Ukraine
OrcID: 0000-0002-0428-9273
wild_miledi@ukr.net

Liliia P. Yurchuk
student
Kyiv National University of Construction and Architecture, Kyiv, Ukraine
OrcID: 0000-0002-4421-3476
lili.yurchyk@gmail.com

Pavlo S. Demianchuk
student
Kyiv National University of Construction and Architecture, Kyiv, Ukraine
OrcID: 0000-0001-5140-9672
demianchuk.pasha2@gmail.com

ANALYSIS OF THE STATE OF CYBER SECURITY IN THE LEADING COUNTRIES OF THE WORLD

Abstract. The article is devoted to the study of trends in cybercrime, which is a threat to the country's information security. The place and role of cybersecurity in the system of national security are determined. The state of the system of protection against cyber attacks in the developed countries of the world, such as France, Japan, China, South Korea and the United Kingdom, was analyzed. The main shortcomings and perspectives of protection of cyberspace are revealed. The use of modern information technologies in state structures, as well as in society in general, proposes solving information security problems as one of the main ones. The economy, logistics and security of the country increasingly depend on the technical infrastructure and its security. To improve the effectiveness of the fight against cybercrime, developed countries have long started the appropriate work needed to create their own cyber security strategy. Incidents in the field of cybersecurity affect the lives of consumers information and many other services and cyber attacks aimed at various objects of infrastructure of electronic communications systems or technological processes management. Modern world trends in the development of cybercrime and the strengthening of cyber attacks indicate an increase in the value of combating it for the further development of society, which in turn predetermines the assignment of certain groups of social relations of the cybersphere to the competence of legal regulation. The current situation with cybercrime requires constant improvement of methods the fight against cybercrime, the development of information systems and methods aimed at ensuring the cyber security of the country. Necessary tasks are the development of a national strategy on cybersecurity, which will include tactical and strategic priorities and tasks in this area for state bodies. So, the issue of cyberspace security, the fight against cybercrime is relevant both at the international level and at the level of the individual country, and therefore needs further consideration.

Keywords: cyberspace; cyber attacks; protection; cyber security; state security.

ISSN 2663 - 4023

REFERENCES

[1].CYBERSECURITY STRATEGY (2018). Retrieved from: https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf
[2].China publishes first national cybersecurity-strategy. Retrieved from: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy.
[3].Cyberspace Administration of China. Retrieved from: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm
[4].China's Cyber Security Law: how prepared are you?. Retrieved from: https://www.controlrisks.com/campaigns/china-business/chinas-cyber-security-law.
[5].Welcome to GCHQ.Pioneering a new kind of security for an ever more complex world. Retrieved from: www.gchq.gov.uk.
[6].Equities process Publication of the UK's process for how we handle vulnerabilities. Retrieved from: www.ncsc.gov.uk/blog-post/equities-process.
[7].Tencent Xuanwu Lab Security. Retrieved from: http://blogstechnet.microsoft.com/msrc/2018/04/20/recognizing-q3-top-5.
[8].A new approach for cyber security in the UK (2016). Retrieved from: https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk.
[9].Kondakova S. Khlaponin Yu. (2019). Cybersecurity in the UK. First impressions. Business and security, 1.