КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (9), 2020
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2020.9.8592
УДК 004

Мальцева Ірина Робертівна
старший науковий співробітник
Військовий інститут інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0001-6073-4637
irenagold2402@gmail.com

Черниш Юлія Олександрівна
старший науковий співробітник
Військовий інститут інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0002-6626-5656
kobernikoi@ukr.net

Чередниченко Олексій Юрійович
старший науковий співробітник
Військовий інститут інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0002-0816-8321
n0ize@ukr.net

КІБЕРБЕЗПЕКА – ОДНА З НАЙВАЖЛИВІШИХ СКЛАДОВИХ ВСІЄЇ СИСТЕМИ ЗАХИСТУ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Анотація. Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу. Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу. Тому цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи. Стаття посвячена дослідженням тенденцій кібернетичної злочинності, що є загрозою інформаційній безпеці нашої держави. Виділено місце та роль кібернетичної безпеки в системі націоналістичної безпеки держави. Було деталізовано становище системи оборони від кібернетичних атак в передових державах світу, таких як Сполучені Штати Америки та Велика Британія. Виявлено головні недоліки та перспективи встановлення захисту кібернетичного простору. Використання сучасних інформаційних технологій у державних структурах, а також у суспільстві в цілому, висуває вирішення проблем інформаційної безпеки в число основних.

Ключові слова: правила кібербезпеки; кіберпростір; кібератаки; захист; кібербезпека; безпека держави;

1. ВСТУП

У сьогоднішньому глобалізованому світі інформація та бази даних є тими унікальними ресурсами без використання та збереження яких неможливе існування і розвиток як сучасної держави, в якості суспільно-політичного утворення, так і виконання суто військових завдань щодо збереження незалежності та захисту країни. За поглядами експертних кіл та аналітиків провідних країн світу, гібридність сучасного збройного конфлікту визначається саме наявністю потужної інформаційної та кібернетичної складової. Доступ до інформації та захист процесів управління стають визначальними факторами досягнення політичних цілей та військової перемоги.

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; 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 вирішальнезначення 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 статті [4] були окреслені проблеми, які існують в системах захисту захисту кіберпростор та основні задачі, які ставить перед собою наша держава. Визначені напрямки захисту від кіберзагроз, захисту кіберпростору та національної безпеки в державах ЄС та Сполучених Штатів Америки.

Мета статті. є висвітлення стану забезпечення захисту кіберпростору в розвинених країнах світу, що дасть змогу проаналізувати проблеми та перспективи розвитку системи захисту кіберпростору. Встановлення правил поведінки кібернетичної безпеки на території ООС.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Ми проживаємо час інформаційного суспільства, коли інформація, технології та телекомунікаційні системи охопили всі сфери діяльності людини, а також держави. В сьогоденні ми більше і більше застосовуємо їх у своїй діяльності. Не є виключенням і Збройні Сили. Слід мати знання та розуміння, які можливості для зловживання дають технології телекомунікації та глобальної комп’ютерної мережі. В сьогодненні жертвами зловмисних дій хакерів стало не лише населення, але й цілі держави. За шкідливою дією та наслідками використання кіберзброю, а власне такий термін все частіше беруть у використання вчені, можна зрівняти до дією зброї масового ураження. Ось тому кібербезпека — є однією з важливих проблематик, що викликає занепокоєння. Швидкість розвитку інформаційних технологій прямо пропорційне

збільшенню потреби в захисті інформаційних та телекомунікаційних систем. Тому не дивно, що уряди розвинених держав та суспільство усього світу знаходяться в пошуках найкращих охоронних заходів та методів для захисту власних даних Інтернет-ресурсів від загроз кібер характеру.

На підтвердження вищесказаних слів, під час проведення зустрічі президентів держав та голів урядів країн — учасниць Північноатлантичного альянсу, яка відбувалась у 2016 році у Варшаві, було підписано вперше в історії договір між ЄС та НАТО про плідну співпрацю у середовищі безпеки, а саме в питаннях гібридних війн та кібернетичних атак [2]. Кіберпростір, на ряду із землею, повітрям, морем і космосом, названо новітнім оперативним простором, а самі кібероперації — однією з основних частин гібридних війн. Найбільшу концентрацію операціям у кіберпросторі надають такі провідні держави світу як Сполучені Штати Америки, Великобританія, Китай та ін. У бюджеті даних країн виділено великі кошти на підтримку кібернетичної частини збройних сил, а також втілюються програми, що забезпечують національну безпеку та захист об'єктів критичної інфраструктури від кібернетичних атак на постійний основі. Оскільки ніхто не може впевнено сказати, що його мережі мають повний захист, а також можуть вистояти проти багатовекторних кібератак, кібербезпека стала одним із пріоритетів розвитку новітньої армії. Одною з причин такого швидкого розвитку підрозділів кібербезпеки стала гібридна війна, яку заснувала та продовжує ведення Росія проти України. Агресор активно користується кібернетичним простором у війні не лише проти України, а й проти інших Країн. Російська Федерація постійно діє на збільшення кількості операцій по кібернетичному шпіонажу та з більшою силою впливає на думку населення в нашій державі, не соромлячись використовувати фейкові новини та відверту пропаганду. Готовна мета таких операцій є розпалювання непорозумінь, хаосу та паніки всередині держави для влаштування власних інтересів.

Шість років тому Росія розпочала проти України гібридну війну. Цей вид війни передбачає, що країна-агресор публічно не має відношення до даного конфлікту та проводить таємні військові операції [4]. Гібридна війна – це ведення військових дій під прикриттям незаконних збройних формувань, і одночасно з тим проводиться використання широкого спектру політико-економічних, а також інформаційних та пропагандистських заходів, з яких, як правило, і власне розпочинається гібридна війна та які її експортують впродовж всього терміну військових дій. Як видно з вище сказаного, всі з перелічених пунктів зараз мають напрямок проти нашої держави. Деякі провідні експерти Заходу не без підстав дають їй назву ще як «війна новітнього покоління» або «війна новітньої генерації».

Російська тактика таких бойових дій має напрямок, перш за все, проти слабких місць нашої держави. Деякі аспекти такої тактики проявлялися ще раніше в Чечні, Молдові, Естонії та Грузії, але в Україні цю тактику Росія не тільки використовує, а й вдосконалює. Також Росія на постійній основі проводить кібероперації проти суб'єктів критичної інфраструктури, приватного сектору, а також інформаційних та телекомунікаційних систем Збройних Сил України. Яскравим прикладом є в той час проста, але широкомасштабна розвідувальна кібернетична операція, що спрямована на приватний сектор, є BugDrop [3]. Вона полягала в отриманні віддаленого доступу до персональної техніки службовців різноманітних структур, внаслідок чого особисті дані та паролі службовців об'єктів критичної інфраструктури, ЗМІ та наукових установ викрадалися й завантажувалися на файлообмінник Dropbox. Доступ до ПК зловмисники отримали за допомогою розсилки користувачам фішингових електронних листів, в яких просили відкрити файл MSWord, що мав в собі зловісний макрос. Так, за

допомогою одного натиску клавіші користувач може поставити під загрозу не лише власні дані, але й дані, які, в разі потрапляння в руки ворога, несуть неоціненну загрозу для України в цілому. Як правило, такі сплановані атаки організовуються не однією особою, а групою хакерів за допомогою організацій, що мають вплив, в тому числі й силових структур. Угруповання, що стоять за цими кібернетичними операціями, можна прирівняти з художником, який пише картину, маючи використанні різноманітні фарби, полотна та стилі. Аналогічно хакери творчо і креативно створюють віруси та нові атаки, використовуючи не лише прогалини системи, але й психологічний стан людей. Щоб запобігти та вирішити цю проблему потрібно постійно проводити діагностування систем шляхом проведення певних тестів, використовувати спеціалізоване обладнання та залучити кваліфікованих фахівців, здатних усунути причини можливих вразливостей. Також треба мати на увазі, що майже всі ми перебуваємо в єдиному мережевому просторі, і якщо навіть звичайний працівник або військовослужбовець постраждає від будь-якого вірусу, то по цьому ланцюжку може статися зараження на всіх рівнях. Саме тому одним із найважливіших аспектів кібернетичної безпеки є проведення тренінгів з працівниками щодо запобігання та протидії кібернетичним атакам.

Проведення кібероперацій досить складно виявити, особливо в разі застосування так званої «логічної бомби», тобто такої загрози, яка може проявитися не одразу, а протягом кількох місяців або навіть років з моменту потрапляння в систему [1]. Тому треба завжди бути дуже пильним при використанні електронної пошти та Інтернету, мінімізувати використання зовнішніх носіїв інформації (USB-флешки, зовнішні жорсткі диски, телефони тощо) й слідкувати, щоб операційна система та антивірус, встановлені на вашому пристрої, були постійно оновленими.

Питання кібернетичної безпеки в зоні проведення антитерористичної операції наразі майже неосвітлене. І правда, навіщо турбуватися про якісь там міфічні кіберзагрози під постійним вогнем артилерії противника? Що поганого, коли хлопці користуються Wi-Fi-роутером чи бездротовим модемом для доступу до Інтернету? Що може якийсь вірус на одному комп'ютері в порівнянні з танком противника?

Але поглянемо на це з іншого боку: скільки життів коштуватиме залп «Граду», або ПТКР, наведений на випромінення цього роутера або модема? А які наслідки потягне карта або схема розташування військ, відправлені із «зараженого» комп'ютера, зі зламаної поштової скриньки або взагалі «братським» поштовиком mail.ru? Таких прикладів можна наводити десятки, якщо не сотні. На жаль, зазвичай ми сприймаємо тільки видимі загрози, залишаючи без уваги небезпеки віртуальні, тим самим даючи ворогові можливість отримувати цінну інформацію. І як би нам не хотілося це визнавати, та він цією можливістю користується, і користується досить ефективно. Кожен з нас бачив у ЗМІ фото перехоплених документів, розпоряджень чи наказів військового спрямування. Так, оприлюднення саме цих матеріалів мало на меті моральний вплив на солдатів та офіцерів Збройних Сил. Але основна маса зібраної інформації використовується для влаштування засідок та нанесення вогневих ударів [4].

Наведемо кілька простих правил, дотримання яких мінімізує ризики витоку інформації та, відповідно, наслідки, які він може спричинити. Виконувати їх нескладно, але вкрай важливо. Це такі правила, як вимкнення геопозиціонування або визначення місцеперебування на всіх пристроях, оновлення антивірусу, постановка сильних паролів, заборона на використання WiFi-роутерів та інтернет-модемів, заборона на завантаження програм та ігор невідомого походження.

Мобільний телефон є найпростішим способом отримання розвідінформації у світі сучасних технологій. Завдяки новітнім засобам розвідки можливо дізнатися не тільки місце, з якого ведуться переговори, але і їхній зміст. Те ж саме стосується і використання транкінгових та інших радіостанцій. Перш за все необхідно розуміти, що деякі компанії (МТС, Life та інші), що надають послуги мобільного зв'язку, повністю або частково належать громадянам сусідньої держави, тому спецслужби Російської Федерації мають вільний доступ до інформації щодо місцезнаходження абонента та змісту переговорів. По-друге, зміною телефону або SIM-картки, при вибутті в зону АТО, неможливо приховати своє місцезнаходження або переговори. Достатньо однієї вечірньої розмови з рідними чи близькими, прослуханої противником, щоб вас ідентифікувати.

Найважливіше, що потрібно пам'ятати, мобільний телефон постійно надсилає сигнали до базової станції. Це дає змогу «бачити» всі телефони, що знаходяться в зоні її дії. А смартфони, до того ж, самостійно підключаються до Інтернету та передають дані. Отже, про приховання пересування, місцезнаходження базового табору або скупчення військових не може бути й мови. А відтак, здійснити прицільний артобстріл зовсім нескладно [2].

Соціальні мережі надають можливість збору інформації про персональні дані особи без її відома не тільки адміністрацією сайта, але й іншими особами, оскільки відстежити збір відповідної інформації в таких системах неможливо.

Не можна надавати інформацію про себе та своїх рідних і близьких, потрібно обмежити коло знайомств у мережі та приховати свою причетність до служби у війську, не розміщувати на своїй сторінці фото-, відеоматеріали. Такі елементарні правила поведінки при користуванні соціальними мережами допоможуть уникнути невиправних наслідків.

Дотримуватися цих правил нелегко, вони напружують і створюють дискомфорт у спілкуванні з рідними. Проте найважливіше, що ці правила допоможуть повернутися нашим військовослужбовцям додому живими.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Висновок, який ми повинні зробити для себе, — це збільшення інвестування в кібербезпеку, щоб запобігати атакам на великі державні й приватні компанії і протистояти намірам дестабілізувати суспільство.

Крім того, кожне суспільство потребує правил, стандартів, норм, положень, інструкцій та інших документів, щоб почувати себе захищеним у кіберпросторі хоча б у правовому відношенні. Зараз з'являються галузеві нормативні документи, що стосуються кіберризиків, зростає інтерес до цієї галузі з боку законодавчих органів. В Україні розробляються стандарти з безпеки для об'єктів критичної інфраструктури. Все частіше лунають заклики до більш активної взаємодії та обміну інформацією, а також до надання обов'язкової звітності про кібератаки для спільної протидії та мінімізації наслідків таких атак. Слід очікувати встановлення обов'язкових вимог у цій сфері. Навіть якщо це і не відбудеться в найближчому майбутньому, загальна атмосфера сьогодні така, що регулюючі органи, державні структури і навіть клієнти хочуть розширити свої знання про кібербезпеку

ISSN 2663 - 4023

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. Богуш, В. Кривуца таА. Кудін, Інформаційна безпека : Термінологічний навчальний довідник. Київ: ООО «Д.В.К.», 2004.

[2] О. Маруненко, "«Зовнішні і внутрішні інформаційні війни у медійному просторі України»",Український науковий журнал «Освіта регіону: політологія, психологія, комунікації», No4, стор. 91-95, 2011.

[3] В. Богуш таО. Юдін,Інформаційна безпека держави, 1st ed. Київ: МК-Прес, 2005.

[4] У. Ільницька, "«Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам»",Політичні науки, No. 1(2), стор. 27-32, 2016.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023

Irina R. Maltseva
Senior Researcher
Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-6073-4637
irenagold2402@gmail.com

Yuliya O. Chernysh
Senior Researcher
Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-6626-5656
kobernikoi@ukr.net

Oleksii Y. Cherednichenko
Senior Researcher
Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-0816-8321
n0ize@ukr.net

CYBER SECURITY IS ONE OF THE MOST IMPORTANT CONSTITUENTS OF THE ENTIRE SYSTEM OF PROTECTION IN THE ARMED FORCES OF UKRAINE

Abstract. The scientific and technological revolution of the early 21st century has caused profound systemic transformations around the world. First of all, due to the combination of advances in the field of advanced information and communication technologies (ICT) with the acquisitions that have emerged from the rapid development of information and telecommunications systems (ITS), fundamentally new global substances have emerged - the information society, as well as the information and cybernetic spaces they have almost unlimited potential and play a leading role in the economic and social development of every country in the world. However, due to the unprecedented proliferation of ICTs and ITSs, the world community has received not only numerous benefits, but also a number of problems caused by the growing vulnerability of the infosphere to third-party cybernetic influences. Therefore, it is only natural for the need to control and further regulate appropriate relationships, and therefore for the immediate creation of a robust cyber security system. Instead, the absence of such a system could lead to the loss of political independence of any state in the world, since it would involve the actual loss of competition by non-military means and the subordination of its national interests to the interests of the opposing party. As these circumstances play an important role in the geopolitical competition of most countries in the world recently, ensuring cybersecurity and harmony in cyberspace has become a major challenge in our information age. The article is devoted to the study of cybercrime trends, which is a threat to the information security of our country. The place and role of cyber security in the nationalist security system of the state are highlighted. The situation of the cyber defense system in the advanced countries of the world, such as the United States of America and the United Kingdom, was detailed. The main shortcomings and prospects of installing cyberspace protection have been identified. The use of modern information technologies in the state structures, as well as in the society as a whole, makes solving the problems of information security one of the main ones.

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

ISSN 2663 - 4023

REFERENCES

[1] V. Bohush, V. Kryvutsa and A. Kudin,Informatsiyna bezpeka :Terminolohichnyy navchal′nyy dovidnyk. Kyiv: OOO «D.V.K.», 2004. (In Ukrainian)
[2] O. Marunenko, "«Zovnishni i vnutrishni informatsiyni viyny u mediynomu prostori Ukrayiny»",Ukrayins′kyy naukovyy zhurnal «Osvita rehionu: politolohiya, psykholohiya, komunikatsiyi», No4, pp. 91-95, 2011. (In Ukrainian)
[3] V. Bohush and O. Yudin,Informatsiyna bezpeka derzhavy, 1st ed. Kyiv: MK-Pres, 2005.(In Ukrainian)
[4] U. Il′nyts′ka, "«Informatsiyna bezpeka Ukrayiny: suchasni vyklyky, zahrozy ta mekhanizmy protydiyi nehatyvnym informatsiyno-psykholohichnym vplyvam»",Politychni nauky, No1(2), pp. 27-32, 2016. [Accessed 26 March 2019]. (In Ukrainian)