7. Mell P., Grance T., The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST, October 20,2011.
8. Glazunova O., Antonenko O. S., *«Economic Effectiveness of Placing the Academic Cloud on Corporate Platforms»*, V International Student Scientific and Practical Conference «Information Technologies: Economics, Engineering, Education», (13–14 November, 2014, m. Kiev). Available at http://it.nubip.edu.ua/mod/data/view.php?d=5&rid=291. Accessed on: February 10, 2018.
9. Sclater N., *«Electronic Education in the Cloud»,* 10th International Journal on Virtual and Individual Learning Management Systems. 1 (1). 10–19, January-March 2010 (in Russian).
10. *Cloud computing*. Available: http: //uk.wikipedia.org/wiki/Chrome_name (in Ukrainian).
11. Gribiuk O., *«Practicum of the use of xmarnic externs in the occite»*, Theory and methodology of the ecclesiastical education. IV. 2013. Available: http://lib.iitta.gov.ua/1111/1/grybyuk-stattya1hmary%2B_Copy.pdf. Accessed on: February 10, 2018 (in Ukrainian).

Mytko Antonina. Benefits and Threats of the Use of the «Academic Cloud» Service in the Educational Activities of Higher Educational Institutions. In this article, the representation of experience of the new information-communication program implementation in the field of training has been researched. The main types of cloud technologies, which reflect the possible directions of using ICT outsourcing for the creation of educational services, are described. It is emphasized that now cloud technologies are integrated into various industrial and scientific fields, which prompts the development of the «academic cloud». The benefits and threats of using the «academic cloud» service in the educational activity of higher educational institutions are determined.

Key words: ICT, education, cloud, cloud technologies, academic cloud, Internet.

Стаття надійшла до редколегії
25.06.2018 р.

УДК 32:004.056.2(73)

Наталія Ничипорчук
Євгенія Вознюк

Секрет успіху США у сфері інформаційної безпеки

У ході дослідження виявлено багато чинників, які сприяли проведенню успішної інформаційної політики США. Серед них виділено нормативно-правове регулювання, удалу політику державних органів й адміністрації президента, інформованість і довіру населення, кібер-страхування й міжнародну співпраця.

Наголошено, що США має потужну законодавчу базу. Початок розвитку інформаційної безпеки закладено ще в першій половині XX ст. Виокремлено, що від адміністрації президента залежить подальший курс усієї держави, тому двоє останніх приділяли багато уваги проблемі кібертероризму. Вони визнавали, що кіберзлочин і кібершпигунство становлять загрозу національній безпеці країни.

Охарактеризовано законодавство США у сфері зовнішньої інформаційної безпеки, що включає сукупність федеральних законів, законів штатів та нормативних актів, які разом створюють правову основу для утворення й здійснення державної політики у сфері інформаційної безпеки. Виокремлено основні з них: «Національну стратегію захисту кіберпростору» (2003), «Огляд з кібербезпеки» (Cyber Security Review, 2009), «Ініціативу зі всеосяжної національної кібербезпеки» (2010), Стратегію кібербезпеки США 2011 р., Закон CISPA 2012 р. («Cyber Intelliggence Sharring and Protection Act»).

Проаналізовано п’ять основних напрямів діяльності з питань інформаційного захисту, які визначає Стратегія: постійний моніторинг і безперервна оцінка загроз та вразливих місць державних інформаційних систем; здійснення національних заходів зі зменшення загроз й уразливості кіберпростору; уживання заходів щодо захисту інформаційних систем органів влади; забезпечення якісної освіти та навчання з питань захисту кіберпростору; співробітництво з питань національної безпеки й безпеки міжнародного кіберпростору.

Доведено, що кібер-страхування стає поширене в межах країни, тим самим зменшує шанси кіберзлочинців на проведення кібератак. Міжнародна співпраця є однією з важливих складових частин забезпечення інформаційної безпеки.

Ключові слова: інформаційна безпека, кібератака, кібер загроза, США, кібербезпека, кіберпростір, кібер-страхування.

Постановка наукової проблеми та її значення. XXI ст. – ера інформаційних технологій. Свобода доступу до інформації та свобода її поширення, підвищення конкурентоспроможності економіки й розширення можливостей її інтеграції у світову систему господарства, підвищення ефективності державного керування – усі ці переваги надає нам користування інформаційно-комунікативними технологіями. Світ стає більш залежним від сучасних технологій.

Технології, соціальні медіа та транзакції через Інтернет відіграють ключову роль у тому, як більшість організацій ведуть бізнес і спілкуються з потенційними клієнтами сьогодні. Утім, зі всіма перевагами глобалізація у сфері інформаційних технологій підвищує ризик зловживань, крадіжок та шахрайства. Світ стає вразливішим до кібератак.

Ефективність інформаційної безпеки будь-якої держави насамперед залежить від досконалості нормативно-правового регулювання діяльності інформаційної системи державних і громадських органів. Законодавство США у сфері зовнішньої інформаційної безпеки включає сукупність федеральних законів, законів штатів та нормативних актів, які разом складають правову основу для утворення й здійснення державної політики у сфері інформаційної безпеки. Законодавство штатів різниться одне від одного, оскільки нормативні акти окремих штатів є досить відмінними.

Розглядаючи положення законодавства США в інформаційній сфері, помітимо, що вони, з одного боку, спрямовані на забезпечення права громадян на інформацію та конфіденційність їхнього приватного життя, а з іншого – на зовнішню інформаційну безпеку. Це свідчить про збалансованість у законодавствах інтересів особи, суспільства та держави.

У лютому 2003 р. в Сполучених Штатах Америки розроблено «Національну стратегію захисту кіберпростору», у якій визначено комплексний підхід до захисту життєво важливих комунікаційних технологій американської нації. Стратегію розроблено за допомогою кваліфікованих у темі інформаційної безпеки спеціалістів.

«Національна стратегія захисту кіберпростору США» спрямована на захист складних і взаємопов'язаних інформаційних систем, які мають життєво важливе значення для сучасного інформаційного суспільства. Загальна мета цього документа – виокремити організаційні завдання й пріоритетність зусиль задля їх досягнення; визначити напрями та кроки, які мають зробити як урядові структури, так і підприємства й приватні користувачі для досягнення безпеки кібернетичного простору США [1].

Визначено основне завдання у сфері кібернетичної безпеки: «запобігання кібернетичним нападам на критичну інфраструктуру, зниження вразливості нації до таких нападів і мінімізацію збитків та часу відновлення».

29 травня 2009 р. оприлюднено «Огляд з кібербезпеки» (Cyber Security Review), що мав на меті «виробити стратегічну основу кібериніціатив Уряду США». У цьому Огляді до ключових завдань керівництва США у сфері кібербезпеки віднесено забезпечення центральної ролі Білого Дому у формуванні кібербезпекової політики, аби продемонструвати аудиторії як усередині США, так і міжнародним партнерам серйозність намірів американського керівництва у сфері кібербезпеки; перегляд законодавства та політики у сфері кібербезпеки; посилення федерального законодавства та відповідальності у сфері кібербезпеки; просування інформаційних проектів державного, регіонального та локального рівнів.

Крім того, у цьому документі окреслено ключові завдання, спрямовані на посилення кібербезпеки США, а саме: підвищити готовність суспільства до кіберзагроз; посилити кібербезпекову освіту, збільшити кількість федеральних працівників із підготовкою у сфері інформаційних технологій; просувати кібербезпеку як важливий елемент відповідальності урядів усіх рівнів.

На початку березня 2010 р. Президентом США затверджено чергову «Ініціативу зі всеосяжної національної кібербезпеки» Ради національної безпеки США, яка складається з дванадцяти загальних положень, реалізація яких дасть змогу захистити країну й уряд від кібератак та хакерів. Ця ініціатива є складовою частиною розділу Воєнної доктрини США, що стосується кібернетичної оборони.

Документом передбачено створення єдиної федеральної мережі, пов'язаної захищеними каналами зв'язку. Зв'язок цієї захищеної мережі має здійснюватися через контрольовані точки доступу. Окрім того, Ініціатива передбачає об'єднання всіх шести наявних у США центрів оперативного реагування

на кіберзлочини з метою підвищення ефективності їхньої діяльності та проведення більш глибокого аналізу хакерських атак.

Також із метою протидії іноземним кібершпигунам документом передбачено створення підрозділів кіберконтррозвідки, яка поширить свій вплив на всі державні органи США, захист таємних внутрішніх мереж Міноборони США від терористичних атак.

Стратегія кібербезпеки США 2011 р., запропонована Президентом США Б. Обамою, якою передбачено право США вживати заходи у відповідь на ворожі дії в кіберпросторі, розглядаючи їх як будь-які інші загрози. Тобто хакерські атаки прирівняні керівництвом США до оголошення війни. У кінці квітня 2012 р. Сенат США прийняв Закон CISPA («Cyber Intelliggence Sharring and Protection Act»), який дасть змогу Уряду США, приватним агентствам безпеки та будь-яким приватним компаніям за наявності підозр про вчинення кіберзлочину отримати доступ до конфіденційної інформації користувачів і комерційних організацій.

Отже, події 11 вересня спричинили трансформацію уявлень як про національну безпеку в цілому, так і про ІБ як її ключову складову. Зокрема, відбулося формування нової парадигми національної безпеки, США, яка грунтується на усвідомленні повної залежності національної інфраструктури від інформаційних систем та мереж країни.

При цьому під кібернетичним тероризмом у США сьогодні розуміють «навмисне руйнування, переривання чи перекручування даних у цифровій формі чи потоків інформації, що має широкомасштабні негативні політичні, релігійні чи ідеологічні наслідки» [4].

Стратегія визначає п’ять основних напрямів діяльності з питань захисту:

1) постійний моніторинг і безперервна оцінка загроз та вразливих місць державних інформаційних систем;

2) здійснення національних заходів зі зменшення загроз та вразливості кіберпростору;

3) уживання заходів щодо захисту інформаційних систем органів влади;

4) забезпечення якісної освіти й навчання з питань захисту кіберпростору;

5) співробітництво з питань національної безпеки та безпеки міжнародного кіберпростору.

У 2017 р. близько 143 млн американців постраждали внаслідок кібератак. Потерпілі складають більшість американського дорослого населення, яке користується Інтернетом. Близько восьми із десяти людей (77 %) зазнали шкоди внаслідок кіберзлочину або ж знають тих, хто зазнав шкоди. У результаті кібератак американські споживачі, які стали жертвами кіберзлочинності, утратили близько 19,4 млрд дол. США, що в середньому становить 96 дол. на одну жертву. Майже 20 год (19,8) американці витрачають на боротьбу з наслідками кіберзлочину [6].

Рис. 1. *Кількість виявлених кібератак у період із 2006 по 2015 р.*

Джерело: [5].

Кількість кібератак зростає з кожним роком. Лише в період із 2006 по 2015 р. цифра збільшилася з 5503 до 77 183. Незважаючи на моторошну статистику, Сполучені Штати Америки активно борються з кіберзлочинністю, намагаються запобігти новим атакам і допомагають населенню впоратися з наслідками. У чому ж секрет такої успішності США у сфері інформаційної безпеки. У ході дослідження виявлено такі чинники, що сприяли проведенню успішної інформаційної політики США:

– нормативно-правове регулювання;
– державні органи;
– інформованість та довіра населення;
– кіберстрахуваня.

Нормативно-правове регулювання – чи не найголовніший двигун ефективності забезпечення інформаційної безпеки будь-якої держави. Американський уряд значну увагу приділяв питанням забезпечення безпеки інформації в державних комп'ютерних системах (закони США «Про комп'ютерну безпеку» та «Про удосконалення інформаційної безпеки»), протидії комп'ютерній злочинності (закони «Про комп'ютерне шахрайство та зловживання» і «Про зловживання комп'ютерами»), регулювання співвідношення прав громадян на отримання інформації (закони «Про свободу інформації» та «Про висвітлення діяльності уряду») та конфіденційності їхнього приватного життя (закон «Про охорону персональних даних»).

Важливим аспектом правового регулювання інформаційної безпеки США є забезпечення конфіденційності приватного життя громадян. Особливу роль у регулюванні цього питання відіграє Закон США «Про охорону персональних даних», який був прийнятий у 1974 р.

Державні структури відіграють важливу роль у забезпеченні інформаційної безпеки. Структура інформаційної безпеки в США є доволі розгалуженою та включає в себе значну кількість компонентів, на кожен із яких покладено відповідні завдання та функції з урахуванням їх компетенції.

Згідно із законом США «Про національну безпеку» від 1947 р., головною відповідальною особою із питань забезпечення національної безпеки загалом та інформаційної безпеки зокрема є Президент США. Він приймає найважливіші рішення із питань національної безпеки країни. Політика інформаційної безпеки в багатьох аспектах залежить від вибраного курсу людини при владі. Так, для прикладу, адміністрація Б. Обами приділяла багато уваги питанням кібербезпеки, виділивши при цьому значні ресурси для боротьби з кібератаками. У бюджеті США на 2016 фінансовий рік кібербезпеку закладено пріоритетом діяльності адміністрації, виділено 14 млн доларів для того, щоб подолати нагальні загрози кібератак [8].

За вирішення окремих питань щодо забезпечення національної безпеки відповідають держсекретар та міністр оборони. Правоохоронні органи США відіграють важливу роль у досягненні цілей кібербезпеки, за допомогою розслідування широкого кола кіберзлочинів – від крадіжки та шахрайства до затримання й переслідування відповідальних осіб. Департамент внутрішньої безпеки (DHS) співпрацює з іншими федеральними установами для проведення кримінальних розслідувань для знешкодження кіберзлочинців, а також займається підготовкою технічних експертів, розробленням стандартизованих методів і нових інструментів протидії кіберзлочинності.

Секретна служба США підтримує цільові групи, які зосереджені на виявленні та пошуку міжнародних кіберзлочинців, пов'язаних із кібератаками, банківським шахрайством й іншими комп'ютерними злочинами. Відділ кіберрозвідки Секретної служби безпосередньо сприяє арештам транснаціональних кіберзлочинців, відповідальних за крадіжку сотень мільйонів номерів кредитних карт і втрату близько 600 млн дол фінансовими й роздрібними установами. Секретна служба також керує Національним комп'ютерним криміналістичним інститутом, який надає працівникам правоохоронних органів, прокурорам та суддям кіберпідготовку та інформацію для боротьби з кіберзлочинністю.

Центр імміграції та митного контролю США (ICE), що включає дослідження національної безпеки (HSI) і Центр кіберзлочинності (C3), надає комп'ютерні технічні послуги для підтримки внутрішніх та міжнародних розслідувань транскордонних злочинів. Центр кіберзлочинності складається з підрозділу з боротьби з кіберзлочинністю, підрозділу з розслідування випадків експлуатації дітей та підрозділу комп'ютерно-технічної експертизи. У C3 також працює повністю обладнана комп'ютерна

лабораторія судово-медичної експертизи, яка спеціалізується на відновленні цифрових доказів і пропонує навчання у сфері комп'ютерно-дослідницької й криміналістичної майстерності [2].

Довіра та обізнаність населення. Незважаючи на кібератаки, населення, зазвичай, продовжує довіряти установам, які впорядковують дані та особисту інформацію в мережі Інтернет. Проте близько 53 % споживачів втратили довіру до свого уряду [6]. Американці прагнуть до цифрової грамотності й бажання її покращити виходить далеко за рамки молодого покоління. Більше восьми з 10 опитаних людей сказали, що хочуть поліпшити свої знання й уміння в цій сфері. Загальні мотиватори для бажання покращити навички цифрової грамотності включають заощадження грошей, інформування й підтримку друзів та сім'ї.

Поліпшення професійних навичок і безпека Інтернету також є головними пріоритетами для міленіалів. Кожен із чотирьох 18–34-річних людей відзначає використання професійного програмного забезпечення як зону, яку вони найбільше прагнуть розвинути, і 24 % тієї ж вікової групи хотіли навчитися безпечно користуватись Інтернетом [3].

Кібер-страхування – захист малого та середнього бізнесу. Кібер-страхування – це страховий продукт, що використовується для захисту бізнесу й окремих користувачів від ризиків, пов'язаних з Інтернетом і в цілому ризиків, пов'язаних з інфраструктурою та діяльністю в галузі інформаційних технологій. Атаки на весь бізнес зростають. Малі підприємства схиляються до думки, що їх ця загроза омине, проте Symantec виявив, що понад 30 % випадків фішингу у 2015 р. простежено в організаціях із 250 працівників. Звіт Symantec про загрози Інтернет-безпеці у 2016 р. засвідчив, що 43 % усіх атак у 2015 р. були спрямовані на малі підприємства [9].

Кібер-страхування не може повністю захистити організацію від кіберзлочинності, але це може втримати бізнес компанії на стабільній фінансовій основі, якщо відбудеться кібератака.

50 % американських фірм не мають страхування від кібер-ризиків і 27 % керівників США кажуть, що їхні компанії не планують узяти кібер-страхування, хоча 61 % із них очікують, що кількість кібер-порушенн збільшиться в наступному році [10]. Водночас можемо прослідкувати позитивну тенденцію за 2016 р.: за цей рік у США виробники заплатили за кібер-страхування 36,9 млн дол., що на 89 % більше, ніж роком раніше.

Ключовими перевагами кіберстрахування є покриття витрат, починаючи від внутрішнього розслідування інциденту відділу інформаційних технологій і кроків, спрямованих на виправлення ситуації з утраченими доходами та заробітною платою.

Страхові поліси зазвичай уключають покриття витрат на реабілітацію репутації компанії: компенсацію клієнтам, постраждалим від інциденту, а також оплату консультантів із кризового менеджменту для надання допомоги у відновленні бренду компанії [7]. Хоча варто зазначити, що послуги кібер-страхування тільки розвиваються.

Висновки й перспективи подальших досліджень. Отже, у ході дослідження виявлено багато чинників, які сприяли проведенню успішної інформаційної політики США. Серед них виділено нормативно-правове регулювання, вдалу політику державних органів та адміністрації президента, інформованість та довіру населення, кібер-страхування та міжнародну співпрацю.

Наголошено, що США має потужну законодавчу базу. Початок розвитку інформаційної безпеки закладено ще в першій половині XX ст. Проаналізовано п'ять основних напрямів діяльності з питань інформаційного захисту, які визначає Стратегія: постійний моніторинг й безперервна оцінка загроз і вразливих місць державних інформаційних систем; реалізація національних заходів зі зменшення загроз та вразливості кіберпростору; здійснення заходів щодо захисту інформаційних систем органів влади; забезпечення якісної освіти й навчання з питань захисту кіберпростору; співробітництво з питань національної безпеки та безпеки міжнародного кіберпростору.

Джерела та література

1. Andress J. The Basics of Information Securit. URL: http://www.sciencedirect.com/science/article/pii/B9781597496537 000013.
2. Combating Cyber Crime. URL: https://www. dhs.gov/topic/combating-cyber-crime.
3. Digital Literacy in 2015: America's Complicated Relationship with the Internet URL: http://www.rasmussen.edu/resources/digital-literacy-in-america/.

4. Larson S. The hacks that left us exposed in 2017. URL: http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/ index.html.
5. Majeed M. Top and Most Impactful Cyber Attacks in the USA. URL: http://blog.externetworks.com/top-cyber-attacks-in-the-usa/.
6. Norton Cyber Security Insights Report 2017 United States Result. URL: http://now.symassets.com/ content/dam/norton/global/pdfs/norton_ cybersecurity_insights/NCSIR-global-results-US.pdf.
7. The benefits of Cyber Insurance. URL: https://www.loricainsurance.com/legacy/documents/Summary_-_ Cyber.pdf.
8. The New US Security Agenda: Trends and Emerging Threats. URL: goo.gl/5C3WiJ.
9. What is cyber insurance and why you need it. URL: https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html.
10. Why 27% of U.S. Firms Have No Plans to Buy Cyber Insurance. URL: https://www.insurancejournal. com/news/national/2017/05/31/ 452647.htm.

Nychyporchuk Natalia, Vozniuk Eugenia. The Secret of US Success in the Field of Information Security. The study found many factors contributing to the successful US information policy. Among them are regulatory legal regulation, successful policy of state bodies and the administration of the president, public awareness and confidence, cyber-insurance and international cooperation.

It is noted that the US has a strong legislative base. The beginning of the development of information security was laid in the first half of the twentieth century. It is emphasized that the further course of the whole state depends on the administration of the president, therefore the two last Presidents paid much attention to the problem of cyber-terrorism. They recognized that cybercrime and cyber-espionage threaten the national security of the country.

The US law on external information security has been described, which includes a set of federal laws, state laws and regulations that together form the legal basis for the formation and implementation of state policy in the field of information security. The main features of the National Cyber Spaces Protection Strategy (2003), Cyber Security Review (2009), the Comprehensive National Cyber Security Initiative (2010), the US Cybersecurity Strategy 2011, the CISPA 2012 Act (Cyber Intelligence Sharring and Protection Act) were highlighted.

The five main directions of activity on information protection issues that are defined by the Strategy are analyzed: constant monitoring and continuous evaluation of threats and vulnerabilities of state information systems; implementation of national measures to reduce the threats and vulnerabilities of cyberspace; implementation of measures to protect the information systems of the authorities; providing quality education and training on issues of protection of cyberspace; cooperation on issues of national security and security of international cyberspace.

It is proved that cyber insurance is becoming widespread within the country, thus reducing the chances of cybercriminals to commit cyber attacks. International cooperation is one of the important components of ensuring information security.

Key words: information security, cyber attack, cyber threat, USA, cyber security, cyberspace, cyber-insurance.

Стаття надійшла до редколегії
09.04.2018 р.

УДК 004.774-047.44

Ярослава Пахольчук

Інструменти веб-аналітики для аналізу відвідувачів сайтів

У статті вказано причини, які зумовлюють необхідність використання засобів веб-аналітики для досягнення бізнес-цілей і збільшення ефективності сайту. Проаналізовано роль веб-аналітики як діяльності, яка спрямована на проведення аналізу користувачів веб-ресурсу. Незважаючи на велику кількість зарубіжних і вітчизняних праць стосовно дослідження веб-аналітики та її інструментів, потрібно констатувати, що в науковій літературі так і не сформовано усталеної, повноцінної дефініції цього поняття. Визначено та схарактеризовано методи веб-