Sławomir Iskierka, Janusz Krzemiński, Zbigniew Weżgowiec

Zagadnienie bezpieczeństwa aplikacji internetowych w programach dydaktycznych

Dydaktyka Informatyki 12, 146-154

2017

Dydaktyka Informatyki 12(2017)
ISSN 2083-3156
DOI: 10.15584/di.2017.12.17
http://www.di.univ.rzeszow.pl

Wydział
Matematyczno-Przyrodniczy UR
Laboratorium Zagadnień
Społeczeństwa Informacyjnego

Sławomir ISKIERKA[1], **Janusz KRZEMIŃSKI**[2], **Zbigniew WEŻGOWIEC**[3]

[1] *Prof. nadzw. dr hab. inż., Politechnika Częstochowska, Wydział Elektryczny, Instytut Informatyki, ul. Armii Krajowej 17, 42-200 Częstochowa; iskierka@el.pcz.czest.pl*
[2] *Dr inż., Politechnika Częstochowska, Wydział Elektryczny, Instytut Informatyki, ul. Armii Krajowej 17, 42-200 Częstochowa; krzem@el.pcz.czest.pl*
[3] *Dr inż., Politechnika Częstochowska, Wydział Elektryczny, Instytut Informatyki, ul. Armii Krajowej 17, 42-200 Częstochowa; wezgow@el.pcz.czest.pl*

ZAGADNIENIE BEZPIECZEŃSTWA APLIKACJI INTERNETOWYCH W PROGRAMACH DYDAKTYCZNYCH

SAFETY ISSUE WEB APPLICATIONS EDUCATIONAL PROGRAMMES

Słowa kluczowe: bezpieczeństwo, aplikacje internetowe, programy dydaktyczne.
Keywords: security, Web-based applications, educational programs.

Streszczenie

W artykule poruszono zagadnienia związane z bezpieczeństwem aplikacji internetowych w aktualnych programach szkolnych. Zwrócono uwagę na fakt, że w związku z dynamicznym rozwojem usług oferowanych przez Internet kwestie bezpieczeństwa aplikacji internetowych stają się kluczowym problemem dla ich twórców. Wskazano na liczne przypadki naruszenia bezpieczeństwa aplikacji internetowych. Przeanalizowano, jak programy nauczania szkół i uczelni wyższych uwzględniają kwestie bezpieczeństwa aplikacji internetowych w trakcie nauki ich tworzenia. Wysunięto wnioski dotyczące kwestii omawiania i nauki bezpieczeństwa aplikacji internetowych we współczesnym procesie dydaktycznym.

Summary

This article discusses problems related to the security of the internet applications in the present school education. A special attention is drawn to the fact, that due to the dynamical development of the services offered via the Internet, security issues of the internet applications have become a major concern for their creators. Numerous cases of security breach in the internet applications are pointed out. It has been analyzed, how the educational programs of both schools and universities include the security issues in the course of making of the internet applications. Conclusions related to the discussion and study of the security of internet applications in the modern educational process are presented.

Wstęp

Internet w ostatnich latach stał się niezwykle popularnym źródłem pozyskiwania informacji i komunikacji międzyludzkiej, a dzięki usługom, które oferuje (praktycznie w każdej dziedzinie życia) jest niezastąpionym składnikiem życia współczesnego człowieka – człowieka ery informacyjnej. Popularność tego medium i przeniesienie do niego wielu codziennych czynności (takich jak opłaty bankowe, poczta elektroniczna, kupno towarów w sklepach internetowych czy wreszcie poszukiwanie pracy) wymaga od użytkownika sieci odpowiednich umiejętności związanych z możliwością korzystania z tych usług, a od projektanta aplikacji internetowych (dzięki którym świadczone są te usługi) wiedzy, która pozwala mu zaprojektować funkcjonalną aplikację. Aplikację, która będzie w pełni spełniała oczekiwania usługobiorcy, a ponadto będzie aplikacją bezpieczną, tzn. taką, której użytkowanie nie spowoduje obecnie i w przyszłości żadnych niepożądanych skutków ubocznych dla programów użytkownika i jego sprzętu.

Napisanie tego typu aplikacji internetowej wymaga odpowiedniej wiedzy merytorycznej dotyczącej zagadnienia, którego dana aplikacja dotyczy oraz wiedzy dotyczącej bezpiecznego jej funkcjonowania w Sieci. Oba te elementy powinny być realizowane podczas nauki programowania aplikacji internetowych (dzisiaj praktycznie każde oprogramowanie jest udostępniane w Sieci). Przegląd aktualnych programów edukacyjnych dotyczących programowania skłania do wniosku, że położony jest w nich właśnie nacisk na naukę czystego programowania, a kwestie związane z bezpieczeństwem projektowanych aplikacji są traktowane drugoplanowo, co przy dzisiejszym funkcjonowaniu aplikacji we współczesnej cyberprzestrzeni wydaje się zjawiskiem wyjątkowo niepokojącym.

Współczesne technologie internetowe cechuje niezwykła dynamika wzrostu. Związane jest to zarówno z pojawianiem się nowych aplikacji z nieznanymi dotąd funkcjonalnościami, które wkraczają coraz głębiej w nasze codzienne życie, jak i niespotykany rozwój infrastruktury teleinformatycznej.

Internet rzeczy, wirtualna rzeczywistość, otwarte zasoby edukacyjne, portale społecznościowe, wszelkiego typu usługi są obecnie oferowane właśnie w Sieci.

Przypadki naruszenia bezpieczeństwa aplikacji internetowych

Podstawową cechą współczesnych aplikacji jest ich usieciowienie, tzn. pisane są z założeniem, że będą funkcjonować w środowisku sieciowym. Najczęściej jest to sieć Internet, rzadziej intranet. W szczególnym przypadku może to być wyizolowana sieć, która nie jest częścią światowego Internetu (np. sieć tajnej instalacji wojskowej, czy sieć wybranych służb specjalnych). Ze względu na charakter niniejszej pracy omawiane zagadnienia dotyczyć będą jedynie Internetu. Sieci wyizolowane rządzą się bowiem swoimi prawami, co nie znaczy, że nie

istnieją sposoby ingerencji w oprogramowanie funkcjonujące na komputerach znajdujących się w tych sieciach[1].

Naruszanie bezpieczeństwa aplikacji internetowych (ataki hackerskie) dawno przestały być domeną pojedynczych osób, które działały z reguły z pobudek finansowych czy ambicjonalnych (pokażę Wam, że się do Was włamię). Obecnie dokonują tego typu ataków zorganizowane grupy przestępcze, służby specjalne czy nawet jak sugerują niektóre informacje medialne rządy poszczególnych państw. Motywy ataków ze strony grup przestępczych mają najczęściej charakter finansowy. Tego typu ataki np. (bardzo obecnie popularne) na komputery szpitali i placówek służby zdrowia z wykorzystaniem oprogramowania ransomware służą przestępcom do uzyskania gratyfikacji finansowych za możliwość odbezpieczenia zaszyfrowanych przez nich danych komputerowych[2].

Udane ataki na popularne serwisy internetowe takie jak LinkedIn, MySpace, Dropboks czy Yahoo świadczą o niezwykłej przebiegłości (wiedzy?) atakujących, którym nie potrafią sprostać nawet najwięksi potentaci internetowi[3].

Niezwykle groźne są ataki na państwową infrastrukturę przemysłową. Za ataki takie obwiniane są w tym przypadku „obce państwa". Przykładem może być tutaj atak na sieć energetyczną Ukrainy[4].

Cyberwojną można nazwać ataki na instalacje wojskowe państw trzecich czy przypuszczalną ingerencję Rosji na wyniki wyborów prezydenckich w USA[5].

Ostatnio (październik 2016 r.) pojawiło się zupełnie nowe zagrożenie. Jak ostrzegają eksperci od bezpieczeństwa sieciowego testowana jest (przez kogo?)

---

[1] *AirHopper – narzędzie do wykradania danych z odizolowanych, odciętych od sieci komputerów*, https://niebezpiecznik.pl/post/airhopper-narzedzie-do-wykradania-danych-z-odizolowanych-odcietych-od-sieci-komputerow/ (dostęp: 20.12.2016 r.).

[2] D. Maikowski, *Groźny wirus sparaliżował sieć szpitali. Cyberprzestępcy stają się coraz bardziej zuchwali?*, http://next.gazeta.pl/next/7,151243,19832143,grozny-wirus-sparalizowal-siec-szpitali-cyberprzestepcy-staja.html#BoxBizImg (dostęp: 20.12.2016 r.); R. Kędzierski, *Zobaczyli to na ekranie monitora i stwierdzili „Lepiej zapłacić okup, niż..."*, http://next.gazeta.pl/internet/1,104530,19657869,hakerzy-zmusili-szpital-do-zaplacenia-okupu-za-dane-pacjentow.html (dostęp: 20.12.2016 r.).

[3] D. Maikowski, *To największy atak w historii Internetu. Wykradziono dane miliarda użytkowników Yahoo,* http://next.gazeta.pl/next/7,151243,21121874,to-najwiekszy-atak-w-historii-internetu-wykradziono-dane-miliarda.html#MTstream (dostęp: 20.12.2016 r.).

[4] *„Milowy krok" w działalności hakerów. Wyłączyli wielką elektrownię*, http://www.tvn24.pl/awaria-elektrowni-na-ukrainie-i-700-tys-domow-bez-pradu,608526,s.html (dostęp: 20.12.2016 r.); *Cyberatak na ukraińską sieć energetyczną. USA pomagają w śledztwie*. http://www.energetyka24.com/291853,cyberatak-na-ukrainska-siec-energetyczna-usa-pomagaja-w-sledztwie (dostęp: 20.12.2016 r.).

[5] *Media: rosyjscy hakerzy przejęli skrzynki najważniejszych wojskowych USA*, http://www.tvn24.pl/cbs-atak-rosyjskich-hakerow-na-wojsko-usa-wlamanie-do-poczty,700287,s.html (dostęp: 20.12.2016 r.); *FBI opublikowała nowy raport oskarżający Rosję o ingerencję w amerykańskie wybory*, http://www.rp.pl/Wybory-w-USA/161239996-FBI-opublikowala-nowy-raport-oskarzajacy-Rosje-o-ingerencje-w-amerykanskie-wybory.html#ap-1 (dostęp: 31.12.2016 r.); *„Rosja musi ponieść konsekwencje przeprowadzania ataków hakerskich",* http://www.tvn24.pl/amerykanski-senator-john-mccain-o-rosyjskich-atakach-hakerskich,703567,s.html (dostęp: 31.12.2016 r.).

możliwość sparaliżowania, czy wręcz wyłączenia Internetu[6]. Próby takie (sparaliżowania Internetu) według firm zajmujących się bezpieczeństwem sieciowym mogą być przeprowadzone już w 2017 roku[7].

W odpowiedzi na te zagrożenia Polska (Ministerstwo Cyfryzacji) przygotowuje strategię dotyczącą cyberbezpieczeństwa państwa[8]. Konsultacje nad tym projektem zostały zakończone 7 października 2016 roku. Strategia ta powinna zostać w miarę szybko przyjęta przez rząd Rzeczypospolitej Polskiej. Minister cyfryzacji ustosunkowując się do tej strategii stwierdziła jednoznacznie, że ministerstwo nie posiada wystarczających środków finansowych, ekspertów ani potrzebnej wiedzy, aby tę strategię realizować[9]. Ponadto ustosunkowując się do ostatniej awarii systemu ePUAP minister stwierdziła: „Tym razem awaria jest za poważna, żeby wystarczyło pogonienie ludzi. Sposób w jaki zbudowano ePUAP może być przedmiotem habilitacji. Pisałam już kiedyś, że gdyby nie środki UE to należałoby go zaorać"[10]. Opnie przedstawione przez minister cyfryzacji należy przyjąć z głębokim zaniepokojeniem.

Wszystkie przedstawione powyżej ataki świadczą o tym, że obecnie kwestie bezpieczeństwa infrastruktury sieciowej i bezpiecznego projektowania aplikacji internetowych winny mieć bezwzględne pierwszeństwo w stosunku do innych zagadnień takich jak między innymi funkcjonalność czy przyjazny użytkownikowi interfejs danej aplikacji.

Nauka bezpiecznego programowania w polskim systemie oświatowym

Doceniając rolę, jaką odgrywa i będzie odgrywała w najbliższych latach umiejętność korzystania przez obywateli ze zdobyczy nowoczesnych technologii teleinformatycznych, wprowadzono do polskiego systemu oświaty naukę pro-

[6] R. Kędzierski, *Eksperci ostrzegają: „Ktoś testuje jak wyłączyć Internet". Wczorajszy atak na USA był największy w historii*, http://next.gazeta.pl/next/7,151243,20874685,eksperci-ostrzegaja-ktos-testuje-jak-wylaczyc-internet-wczorajszy.html#Czolka3Img (dostęp: 31.12.2016 r.); *Duży atak DDoS powoduje problemy z dostępem do wielu usług*, https://zaufanatrzeciastrona.pl/post/duzy-atak-ddos-powoduje-problemy-z-dostepem-do-wielu-uslug/ (dostęp: 31.12.2016 r.).

[7] R. Kędzierski, *Ktoś przygotowuje się właśnie do globalnego ataku na Internet. Narzędzia są już gotowe do użycia*, http://next.gazeta.pl/next/7,151243,21175370,ktos-przygotowuje-sie-do-globalnego-ataku-na-internet-specjalisci.html#BoxBiz#BoxBizCzZ20 (dostęp: 31.12.2016 r.).

[8] *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020, _v_29_09_2016*, https://mc.gov.pl/konsultacje/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rp-na-lata-2016 (dostęp: 31.12.2016 r.).

[9] D. Maikowski, *Minister Streżyńska właśnie przyznała, że nie ma pieniędzy i ludzi, by zapewnić Polsce bezpieczeństwo*, http://next.gazeta.pl/next/7,151243,20829529,minister-strezynska-wlasnie-przyznala-ze-nie-ma-pieniedzy-i.html#BoxBizImg (dostęp: 31.12.2016 r.).

[10] D. Maikowski, *Kompromitacji ePUAP ciąg dalszy. Ministerstwo: Wciąż nie wiemy, kiedy system zostanie naprawiony*, http://next.gazeta.pl/next/7,151243,20041148,powazna-awaria-systemu-epuap-strezynska-gdyby-nie-srodki.html (dostęp: 31.12.2016 r.).

gramowania na wszystkich etapach kształcenia. Pilotażowy program tej nauki został wprowadzony we wrześniu 2016 roku i objął prawie 1600 szkół[11]. Od września 2017 roku nauka programowania będzie już realizowana w normalnym cyklu kształcenia począwszy od pierwszej klasy szkoły podstawowej. Jak ważną funkcję spełniają technologie teleinformatyczne w życiu współczesnego społeczeństwa można prześledzić m.in. w pracy W. Piecucha[12].

Obecnie, tj. na przełomie roku 2016 i 2017 dyskusja o nauce programowania w tym programowania bezpiecznych aplikacji internetowych w polskim systemie oświatowym jest bardzo utrudniona. Związane jest to z zapowiadaną przez MEN reformą edukacji polegającą na likwidacji szkół gimnazjalnych i przywrócenia dawnego systemu szkolnictwa opartego na 8-letniej szkole podstawowej, 4-letnim liceum ogólnokształcącym, 5-letnim technikum oraz dwustopniowych szkołach branżowych[13]. Dodatkowo dyskusja ta, z konieczności, musi dotyczyć projektów rozporządzeń dotyczących podstaw programowych i ramowych planów nauczania, pomimo że prezydent RP nie podpisał jeszcze Prawa oświatowego likwidującego gimnazja[14]. Należy również nadmienić, że obecnie obowiązuje podstawa programowa wprowadzona rozporządzeniem ministra edukacji narodowej z dnia 23 czerwca 2016 roku[15].

Analizując przedstawione podstawy programowe (nie wnikając w ich status prawny) należy stwierdzić, że kwestie bezpiecznego projektowania aplikacji internetowych zostały potraktowane dość pobieżnie. Podstawa programowa z informatyki – szkoła podstawowa jako V cel kształcenia informatycznego (dla wszystkich etapów edukacyjnych) – Przestrzeganie prawa i zasad bezpieczeństwa zawiera tylko takie elementy jak: respektowanie prywatności informacji i ochrony danych, prawa własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocenę zagrożeń związanych z technologią i ich

[11] *Nauka programowania i szerokopasmowy Internet dla szkół!*, https://men.gov.pl/ministerstwo/informacje/nauka-programowania-i-szerokopasmowy-internet-dla-szkol.html (dostęp: 31.12.2016 r.); *Cyfryzacja szkół – podsumowanie działań Ministerstwa Edukacji Narodowej i Ministerstwa Cyfryzacji*, https://men.gov.pl/ministerstwo/informacje/cyfryzacja-szkol-podsumowanie-dzialan-ministerstwa-edukacji-narodowej-i-ministerstwa-cyfryzacji.html (dostęp: 31.12.2016 r.).

[12] A. Piecuch, *Edukacja informatyczna na początku trzeciego tysiąclecia*, Rzeszów 2008.

[13] *Będzie likwidacja gimnazjów, Sejm przegłosował reformę oświaty. Opozycja: „najczarniejszy dzień polskiej edukacji"*, http://wiadomosci.gazeta.pl/wiadomosci/7,114884,21121667,bedzie-likwidacja-gimnazjow-sejm-przeglosowal-reforme-oswiaty.html#MT2 (dostęp: 31.12.2016 r.).

[14] https://men.gov.pl/projekty-ramowych-planow-nauczania (dostęp: 31.12.2016 r.); J. Suchecka, *MEN wyprzedził podpis prezydenta. Nowe podstawy programowe już opublikowane*, http://wyborcza.pl/7,75398,21187034,men-wyprzedzil-podpis-prezydenta-nowe-podstawy-programowe-juz.html#BoxGWImg (dostęp: 31.12.2016 r.).

[15] Rozporządzenie ministra edukacji narodowej z dnia 17 czerwca 2016 r. zmieniające rozporządzenie w sprawie podstawy programowej wychowania przedszkolnego oraz kształcenia ogólnego w poszczególnych typach szkół, Dz.U. z 2016 r., poz. 895, http://dziennikustaw.gov.pl/du/2016/895 (dostęp: 16.12.2016 r.).

uwzględnienie dla bezpieczeństwa swojego i innych[16]. Dla uczniów szkół podstawowych są to może informacje wystarczające niemniej autorzy uważają, że już na tym etapie nauki informatyki należałoby wprowadzić (sygnalnie!?) kwestie związane z bezpieczeństwem projektowania aplikacji internetowych.

Podstawy programowe dla pozostałych typów szkół (obecnie jest grudzień 2016 r.) będą dopiero opracowane, więc dyskusja na temat zawartych (w przyszłości) w nich elementów dotyczących bezpiecznego projektowania aplikacji internetowych jest przedwczesna. Niemniej autorzy proponują, aby były one w nich zdecydowanie uwypuklone.

Nowoczesne i aktualne podstawy programowe są warunkiem koniecznym, ale niewystraczającym, by wprowadzać do polskiego systemu oświatowego skuteczny system nauczania informatyki, a w tym nauki bezpiecznego projektowania aplikacji internetowych. Aby robić to efektywnie potrzebni są doskonale wykształceni i posiadający wysokie umiejętności praktyczne nauczyciele oraz niezbędna jest odpowiednia baza sprzętowa (komputery i szybkie sieci szerokopasmowe) będąca na wyposażeniu szkół.

W celu przygotowania nauczycieli do trudnych, stojących przed nimi zadań kuratorzy oświaty zorganizowali wiele konferencji szkoleniowych oraz ufundowali granty dla nauczycieli na opracowanie nowych programów nauczania[17]. Szkoły wyższe przygotowały natomiast studia podyplomowe, na których nauczyciele mogą podwyższać swoje kwalifikacje[18].

Jak nauczyciele wykorzystują nowoczesne technologie teleinformacyjne w swojej pracy dydaktycznej przedstawiono m.in. w raporcie E. Baron-Polańczyk[19].

Baza dydaktyczna szkół będzie unowocześniona o nowe komputery oraz zostaną one podłączone do szerokopasmowego Internetu w związku z przyjęciem przez rząd w dniu 8 stycznia 2014 r. Narodowego Planu Szerokopasmowego[20]. Główne cele tego planu to zapewnienie do roku 2020: powszechnego dostępu do Internetu o prędkości co najmniej 30 Mb/s i doprowadzenie do wykorzystania usług dostępu o prędkości co najmniej 100 Mb/s przez 50% gospo-

[16] *Podstawa programowa z informatyki, szkoła podstawowa*, https://men. gov.pl/wp-content/uploads/2016/11/podstawa-programowa-z-informatyki-szkola-podstawowa.pdf (dostęp: 31.12.2016 r.).

[17] *Cyfryzacja szkół – podsumowanie działań Ministerstwa Edukacji Narodowej i Ministerstwa Cyfryzacji*, https://men.gov.pl/ministerstwo/informacje/cyfryzacja-szkol-podsumowanie-dzialan-ministerstwa-edukacji-narodowej-i-ministerstwa-cyfryzacji.html (dostęp: 31.12.2016 r.).

[18] http://staff.ii.pw.edu.pl/podyp/sp-NA.htm (dostęp: 31.12.2016 r.); http://www.rekrutacja.uni.wroc.pl/kierunek.html?id=9698#zasady (dostęp: 31.12.2016 r.); http://www.podyplomowe.ur.edu.pl/?id=studia&ids=58 (dostęp: 31.12.2016 r.).

[19] E. Baron-Polańczyk, *Osiągnięcia i niepowodzenia nauczycieli w obszarze wykorzystania ICT (Raport z badań)* [w:] *Edukacja a nowe technologie w kulturze, informacji i komunikacji*, red. D. Siemieniecka, Toruń 2015, s. 209 i nast.

[20] Narodowy Plan Szerokopasmowy, Ministerstwo Administracji i Cyfryzacji, https://mac.gov.pl/files/narodowy_plan_szerokopasmowy_-_08.01.2014_przyjety_przez_rm.pdf (dostęp: 12.12.2016 r.).

darstw domowych[21]. Ponadto w ramach środków z Osi 1 Programu Operacyjnego Polska Cyfrowa Ministerstwo Cyfryzacji ma zadbać o to, by z dotacji unijnych część szkół mogła być podłączona do szerokopasmowego Internetu o szybkości powyżej 100 Mb/s[22]. Planowane jest również stworzenie nowoczesnej Ogólnopolskiej Sieci Edukacyjnej (OSE)[23]. W myśl założeń projektowych, sieć ta ma być siecią teleinformatyczną łączącą wszystkie szkoły w Polsce. Uruchomienie tej sieci pozwoli na wprowadzenie nowych form kształcenia i wyrównanie szans edukacyjnych wszystkich uczniów w Polsce[24].

Zakończenie

Rozwijanie we współczesnym społeczeństwie umiejętności w zakresie wykorzystywania technologii informacyjno-komunikacyjnych, w których nauka programowania stanowi wyższy poziom wtajemniczenia jest obecnie niezbędne. Wynika to z faktu cyfryzującego się rynku pracy, rozwoju usług internetowych, możliwości natychmiastowego pozyskiwania w sieci dowolnej informacji i komunikowania się między sobą, na niespotykaną dotychczas skalę, członków społeczeństwa informacyjnego. Te wszystkie zalety współczesnego zcyfryzowanego świata mają jednak jedną podstawową wadę, są zależne od sprawnej i bezpiecznej sieci (Internetu). Sieci, która może być, jak pokazują liczne tego przykłady szybko i skutecznie zaatakowana (zablokowana). Przy czym atakującymi mogą być organizacje przestępcze, służby specjalne, wojsko czy też rządy obcych państw. Na tego typu ataki zwykły obywatel nie jest przygotowany. Co więcej, nie jest na nie również przygotowana większość programistów, którzy zajmują się tworzeniem aplikacji internetowych. Stworzyć bowiem działającą aplikację internetową, ale przy tym bezpieczną na wszelkiego typu ataki to poważne wyzwanie dla programisty. Umiejętności, jakie powinien on przy tym posiadać są niedostępne dla przeciętnego projektanta aplikacji internetowych i ten fakt winien być uświadamiany wszystkim projektantom.

Ponadto otwarte pozostaje pytanie, jak Polska, w tym polski system oświaty, jest przygotowany na „wyłączenie" Internetu (z różnych przyczyn) na kilka minut, kilka godzin, kilka dni, kilka miesięcy i dłużej?

---

[21] Tamże.

[22] *Cyfryzacja szkół – podsumowanie działań Ministerstwa Edukacji Narodowej i Ministerstwa Cyfryzacji*, https://men.gov.pl/ministerstwo/informacje/cyfryzacja-szkol-podsumowanie-dzialan-ministerstwa-edukacji-narodowej-i-ministerstwa-cyfryzacji.html (dostęp: 31.12.2016 r.).

[23] *Ogólnopolska sieć edukacyjna – założenia do projektu ustawy*, https://men.gov.pl/ministerstwo/informacje/ogolnopolska-siec-edukacyjna-zalozenia-do-projektu-ustawy.html (dostęp: 31.12.2016 r.).

[24] Tamże.

Bibliografia

AirHopper – narzędzie do wykradania danych z odizolowanych, odciętych od sieci komputerów, https://niebezpiecznik.pl/post/airhopper-narzedzie-do-wykradania-danych-z-odizolowanych-odcietych-od-sieci-komputerow/ (dostęp: 20.12.2016 r.).

Baron-Polańczyk E., *Osiągniecia i niepowodzenia nauczycieli w obszarze wykorzystania ICT (Raport z badań)* [w:] *Edukacja a nowe technologie w kulturze, informacji i komunikacji*, red. D. Siemieniecka, Toruń 2015.

Będzie likwidacja gimnazjów, Sejm przegłosował reformę oświaty. Opozycja: „najczarniejszy dzień polskiej edukacji”, http://wiadomosci.gazeta.pl/wiadomosci/7,114884,21121667,bedzie-likwidacja-gimnazjow-sejm-przeglosowal-reforme-oswiaty.html#MT2 (dostęp: 31.12.2016 r.).

Cyberatak na ukraińską sieć energetyczną. USA pomagają w śledztwie, http://www.energetyka24.com/291853,cyberatak-na-ukrainska-siec-energetyczna-usa-pomagaja-w-sledztwie (dostęp: 20.12.2016 r.)

Cyfryzacja szkół – podsumowanie działań Ministerstwa Edukacji Narodowej i Ministerstwa Cyfryzacji, https://men.gov.pl/ministerstwo/informacje/cyfryzacja-szkol-podsumowanie-dzialan-ministerstwa-edukacji-narodowej-i-ministerstwa-cyfryzacji.html (dostęp: 31.12.2016 r.).

Duży atak DDoS powoduje problemy z dostępem do wielu usług, https://zaufanatrzeciastrona.pl/post/duzy-atak-ddos-powoduje-problemy-z-dostepem-do-wielu-uslug/ (dostęp: 31.12.2016 r.).

FBI opublikowała nowy raport oskarżający Rosję o ingerencję w amerykańskie wybory, http://www.rp.pl/Wybory-w-USA/161239996-FBI-opublikowala-nowy-raport-oskarzajacy-Rosje-o-ingerencje-w-amerykanskie-wybory.html#ap-1 (dostęp: 31.12.2016 r.).

http://staff.ii.pw.edu.pl/podyp/sp-NA.htm (dostęp: 31.12.2016 r.).

http://www.podyplomowe.ur.edu.pl/?id=studia&ids=58 (dostęp: 31.12.2016 r.).

http://www.rekrutacja.uni.wroc.pl/kierunek.html?id=9698#zasady (dostęp: 31.12.2016 r.).

https://men.gov.pl/projekty-ramowych-planow-nauczania (dostęp: 31.12.2016 r.).

Kędzierski R., *Eksperci ostrzegają: „Ktoś testuje jak wyłączyć Internet”. Wczorajszy atak na USA był największy w historii*, http://next.gazeta.pl/next/7,151243,20874685,eksperci-ostrzegaja-ktos-testuje-jak-wylaczyc-internet-wczorajszy.html#Czolka3Img (dostęp: 31.12.2016 r.)

Kędzierski R., *Ktoś przygotowuje się właśnie do globalnego ataku na Internet. Narzędzia są już gotowe do użycia*, http://next.gazeta.pl/next/7,151243,21175370,ktos-przygotowuje-sie-do-globalnego-ataku-na-internet-specjalisci.html#BoxBiz#BoxBizCzZ20 (dostęp: 31.12.2016 r.).

Kędzierski R., *Zobaczyli to na ekranie monitora i stwierdzili „Lepiej zapłacić okup, niż...”*, http://next.gazeta.pl/internet/1,104530,19657869,hakerzy-zmusili-szpital-do-zaplacenia-okupu-za-dane-pacjentow.html (dostęp: 20.12.2016 r.).

Maikowski D., *Groźny wirus sparaliżował sieć szpitali. Cyberprzestępcy stają się coraz bardziej zuchwali?*, http://next.gazeta.pl/next/7,151243,19832143,grozny-wirus-sparalizowal-siec-szpitali-cyberprzestepcy-staja.html#BoxBizImg (dostęp: 20.12.2016 r.).

Maikowski D., *Kompromitacji ePUAP ciąg dalszy. Ministerstwo: Wciąż nie wiemy, kiedy system zostanie naprawiony*, http://next.gazeta.pl/next/7,151243,20041148,powazna-awaria-systemu-epuap-strezynska-gdyby-nie-srodki.html (dostęp: 31.12.2016 r.).

Maikowski D., *Minister Streżyńska właśnie przyznała, że nie ma pieniędzy i ludzi, by zapewnić Polsce bezpieczeństwo*, http://next.gazeta.pl/next/7,151243,20829529,minister-strezynska-wlasnie-przyznala-ze-nie-ma-pieniedzy-i.html#BoxBizImg (dostęp: 31.12.2016 r.).

Maikowski D., *To największy atak w historii Internetu. Wykradziono dane miliarda użytkowników Yahoo*, http://next.gazeta.pl/next/7,151243,21121874,to-najwiekszy-atak-w-historii-internetu-wykradziono-dane-miliarda.html#MTstream (dostęp: 20.12.2016 r.).

Media: rosyjscy hakerzy przejęli skrzynki najważniejszych wojskowych USA, http://www.tvn24.pl/ cbs-atak-rosyjskich-hakerow-na-wojsko-usa-wlamanie-do-poczty,700287,s.html (dostęp: 20.12.2016 r.).

„Milowy krok” w działalności hakerów. Wyłączyli wielką elektrownię, http://www.tvn24.pl/awaria-elektrowni-na-ukrainie-i-700-tys-domow-bez-pradu,608526,s.html (dostęp: 20.12.2016 r.).

Narodowy Plan Szerokopasmowy, Ministerstwo Administracji i Cyfryzacji, https://mac.gov.pl/files/narodowy_plan_szerokopasmowy_-_08.01.2014_przyjety_przez_rm.pdf (dostęp: 12.12.2016 r.).

Nauka programowania i szerokopasmowy Internet dla szkół!, https://men.gov.pl/ministerstwo/informacje/nauka-programowania-i-szerokopasmowy-internet-dla-szkol.html (dostęp: 31.12.2016 r.).

Ogólnopolska sieć edukacyjna – założenia do projektu ustawy, https://men.gov.pl/ministerstwo/informacje/ogolnopolska-siec-edukacyjna-zalozenia-do-projektu-ustawy.html (dostęp: 31.12.2016 r.).

Piecuch A., *Edukacja informatyczna na początku trzeciego tysiąclecia*, Rzeszów 2008.

Podstawa programowa z informatyki, szkoła podstawowa, https://men.gov.pl/ wp-content/uploads/2016/11/podstawa-programowa-z-informatyki-szkola-podstawowa.pdf (dostęp: 31.12.2016 r.).

„Rosja musi ponieść konsekwencje przeprowadzania ataków hakerskich”, http://www.tvn24.pl/amerykanski-senator-john-mccain-o-rosyjskich-atakach-hakerskich,703567,s.html (dostęp: 31.12.2016 r.).

Rozporządzenie ministra edukacji narodowej z dnia 17 czerwca 2016 r. zmieniające rozporządzenie w sprawie podstawy programowej wychowania przedszkolnego oraz kształcenia ogólnego w poszczególnych typach szkół, Dz.U. z 2016 r., poz. 895, http://dziennikustaw.gov.pl/du/2016/895 (dostęp: 16.12.2016 r.).

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020, _v_29_09_2016, https://mc.gov.pl/konsultacje/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rp-na-lata-2016 (dostęp: 31.12.2016 r.).

Suchecka J., *MEN wyprzedził podpis prezydenta. Nowe podstawy programowe już opublikowane*, http://wyborcza.pl/7,75398,21187034,men-wyprzedzil-podpis-prezydenta-nowe-podstawy-programowe-juz.html#BoxGWImg (dostęp: 31.12.2016 r.).