***Андрєєва О.М.*[*], *Мусієнко К.*[**]**

КІБЕРЗБРОЯ ТА АНАЛІЗ ЇЇ ДЕСТРУКТИВНОЇ ДІЯЛЬНОСТІ НА ПРИКЛАДІ ВПЛИВУ ВІРУСУ НОВОГО ПОКОЛІННЯ STUXNET НА ІРАНСЬКУ ЯДЕРНУ ПРОГРАМУ

Эта статья о ежедневно возрастающем влиянии информационных технологий на государственные структуры и национальную безопасность. Проблема кибер–безопасности раскрывается путем изучения последствий внедрения вируса нового поколения Stuxnet в компьютерную систему атомной электростанции в Бушере.

Ключевые слова: кибероружие, Stuxnet, кибершпионаж, информационные технологии, кибертерроризм.

У цій статті мова йде про постійно зростаючий вплив інформаційних технологій на державні структури та національну безпеку країни. Проблема кібер–безпеки розкривається шляхом вивчення наслідків впровадження вірусу нового покоління Stuxnet в комп'ютерну систему атомної електростанції в Бушері.

Ключові слова: кіберзброя, Stuxnet, кібершпигунство, інформаційні технології, кібертероризм.

This article is about the daily increasing influence of information technology on government agencies and national security. The problem of cyber security is revealed by studying the effect of introducing a new generation of virus called Stuxnet into the computer system of nuclear power plant in Bushehr.

Keywords: cyber weapons, Stuxnet, cyber espionage, information technology, cyber terrorism.

Актуальність дослідження. В сучасному світі, в якому дедалі більшу роль в житті держави, її економіці та системі безпеки, відіграють кіберпростір та сучасні інформаційні технології, не можна обійти увагою ті загрози, які пов'язані з застосуванням цих високих технологій. У цьому зв'язку все частіше можна почути такі слова, як «кібершпигунство» та «кібервійна».

На сьогоднішній день створення вірусів, троянів і блокування доступу представляються більш простими і дешевими засобами, ніж використання фізичної зброї; в той же час інформаційні атаки можуть завдати справжньої шкоди. Потенційними цілями кібератак можуть ставати системи контролю та комунікацій життєво і стратегічно важливих об'єктів: ядерної і хімічної промисловості, фінансової, продовольчої та енергетичної сис-

[*] доктор політичних наук, доцент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

[**] студентка 3 курсу спеціальності «міжнародна інформація» Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

теми, охорони здоров'я, дорожнього руху, транспортних мереж, уряду, поліції і армії. Таким чином, цілком обґрунтовано можна зробити висновок про те, що ми живемо в епоху легалізації кібернетичної зброї на державному рівні.

Отже, забезпечення безпеки інформаційних і комунікаційних систем сьогодні стає складовою частиною оборонної стратегії будь–якої держави, перетворюючись у «п'яту сферу» війни – поряд із сушею, морем, повітрям і космосом

Метою дослідження є з'ясування специфіки структури вірусу нового покоління Stuxnet, а також встановлення реальних наслідків та впливу його діяльності на Іранську ядерну програму.

У статті була зроблена спроба дослідити структуру вірусу Stuxnet, встановити його характерні відмінності та специфіку; проаналізувати збитки ядерної програми Ірану, внаслідок впровадження даного вірусу на АЕС в Бушері та на основі проведеного дослідження, надати прогнози щодо основних тенденції 2011 року.

Наприкінці вересня стало відомо, що вірус Stuxnet завдав серйозної шкоди іранській ядерній програмі. Використовуючи уразливі місця операційної системи і горезвісний «людський фактор», Stuxnet успішно вразив 1368 з 5000 центрифуг на заводі зі збагачення урану в Натанзі, а також зірвав терміни запуску ядерної АЕС в Бушері. Замовник – невідомий. Виконавець – недбайливий співробітник Siemens, який вмонтував інфікований флеш–накопичувач в робочу станцію. Збиток, нанесений ядерним об'єктам Ірану, можна порівняти зі шкодою від атаки ізраїльських ВПС.

Світ заговорив про війни нового покоління. Кібернетичні атаки можуть стати ідеальними інструментами наступних воєн – вони стрімкі, ефективні у своїй руйнівній силі і, як правило, анонімні. Сьогодні держави в терміновому порядку домовляються про спільні стратегії протистояння кібернетичним загрозам.

Над розгадкою Stuxnet – вірусу, що уразив ядерні об'єкти Ірану – б'ються експерти найрізноманітніших напрямів: від IT–безпеки до лінгвістики та антропології. Stuxnet був виявлений антивірусними лабораторіями досить давно, ще понад два роки тому, проте про справжні масштаби зараження світ дізнався в кінці вересня 2010 року, коли стало відомо про затримку запуску першої в Ірані Бушерської АЕС. Цікавим є той факт, що Stuxnet був виявлений не в Америці, Китаї чи Європі, де більше всього користувачів мережі Інтернет, і де нормальним вірусам сама благодать, а в Ірані. 60% заражень відбулося в державі ісламської революції [1].

Незважаючи на те, що Алі Акбар Салехі, глава Організації з атомної енергії Ірану, заявив, що затримка з пуском АЕС ніяк не пов'язана з діяльністю вірусу [2], Марк Фітцпатрік, співробітник Міжнародного інституту стратегічних досліджень, відзначив, що ця заява «не є переконливою», а також, Іран схильний замовчувати реальні проблеми на АЕС. Через деякий час «проговорився» Махмуд Джафарі, менеджер відділу проектів станції в Бушері. За його словами, Stuxnet «вразив кілька комп'ютерів, але не завдав якоїсь шкоди основній операційній системі станції». Ядерні об'єкти Ірану в Натанзі також постраждали досить серйозно: 1368 з 5000 центрифуг були виведені з ладу в результаті дій Stuxnet. Коли Махмуда Ахмадінеджада після сесії Генасамблеї ООН прямо запитали про технологічні проблеми з ядерною програмою, він лише знизав плечима і нічого не відповів. Також слід зазначити, що за даними New York Times, збиток від дій вірусу в Ірані відкинула ядерну програму країни принаймні на два роки назад [1; 3].

З цілком зрозумілих причин розробники Stuxnet воліють триматися в тіні, проте абсолютно очевидно, що складність вірусу можна назвати безпрецедентною. Так що ж саме робить вірус Stuxnet таким особливим та руйнівним за своїми наслідками? Про військові

цілі вірусу говорить Євген Касперський, генеральний директор «Лабораторії Касперського»: «Stuxnet не краде гроші, не шле спам і не краде конфіденційну інформацію. Цей паразит створений, щоб контролювати виробничі процеси, в буквальному сенсі керувати величезними виробничими потужностями. У недалекому минулому ми боролися з кібер–злочинцями та інтернет–хуліганами, тепер, боюся, настає час кібертероризму, кіберзброї і кібервійн» [4].

Щодо ж до самої структури вірусу, New York Times відзначає, що Stuxnet складається з двох основних компонентів, перший з яких змушує центрифуги працювати в позаштатному режимі, а другий передає неправдиві дані про нормальну роботу. Але саме «сенсаційне» у роботі цього вірусу є то, що він не розсилає спам, не форматує диск і навіть не краде банківські дані. Він цілеспрямовано займається шкідництвом на виробництві. Точніше, він атакує індустріальні системи контролю та управління, які використовують програмне забезпечення під назвою Simatic WinCC. Stuxnet приховано прописує себе на програмовані чіпи (їх використовують для контролю за виробництвом), маскується і вбиває якийсь важливий, невипадковий процес і замість нього повертає певний код. На жаль, що цей код означає, поки невідомо. Також ще однією особливістю цього вірусу є неможливість поширення через мережі. Це, до речі, пояснює спосіб поширенням через флеш–накопичувачі – промислові системи рідко підключені до Глобальної Мережі. Експерт з кіберцентру НАТО в Естонії Кеннет Гірс на одній з конференцій про безпеку висловив припущення, що успіх атаки Stuxnet залежав виключно від контактів з потрібними з людьми і елементарних USB–накопичувачів [3]. «Можна заплатити комусь, хто запустить трояна в закриту систему, або підмінити флешку, яка призначалася тільки для внутрішнього користування», – розмірковує Гірс. – «Досить вставити в стандартний USB–роз'єм комп'ютера інфіковану флешку, і Stuxnet відразу автоматично перескакує на операційну систему, і ніякі антивірусні програми та інші заходи захисту їй не перешкода» [4; 7].

І дійсно, «слабкою ланкою» виявився людський чинник – Stuxnet був занесений в систему за допомогою звичайного USB–накопичувача, який з необережності вставив в робочу станцію недбайливий працівник. Примітно, що після заяв міністра розвідки Ірану Гейдара Мослехі про затримання «ядерних шпигунів» (ними виявилися абсолютно непричетні російські техніки), керівництво Siemens визнало, що вірус занесли співробітники компанії, підкресливши ненавмисний характер зараження. Слід зазначити, що Stuxnet вражає лише конкретний тип контролерів Siemens, а саме SIMATIC S7, який, за даними МАГАТЕ, використовується Іраном [5].

На цьому етапі вже можна зробити певний висновок, що створення подібного проекту потребує величезних інтелектуальних і фінансових інвестицій, а значить, під силу лише структурам масштабу державних. Всі експерти сходяться на думці, що вірус не є результатом зусиль «групи ентузіастів». Лоран Есло, керівник відділу систем безпеки Symantec припускає, що над створенням Stuxnet працювали, як мінімум, від шести до десяти чоловік протягом шести–дев'яти місяців. Франк Рігер, технічний директор GSMK підтримує свого колегу – за його словами, вірус створювала команда з десяти досвідчених програмістів, а розробка зайняла близько півроку. Рігер називає і орієнтовну суму створення Stuxnet: вона становить не менш $ 3 млн. Також більшість експертів сходяться на думці, щодо цілеспрямованості створення даного вірусу [6].

У процесі аналізу Stuxnet деякі ЗМІ зробили висновок, що за створенням вірусу стоїть Ізраїль. Першим заговорив про причетність Ізраїлю до атаки сам Іран. Разом з тим слід підкреслити, що ще минулого літа (нагадаємо, поширення Stuxnet почалося в 2009 р.) ресурс WikiLeaks повідомив про серйозну ядерну аварію в Натанзі. Незабаром після цього

стало відомо, що глава Організації з атомної енергії Ірану Голам Реза Агазаде пішов у відставку без пояснення причин[6]. Приблизно в цей же час в ЗМІ з'явилися висловлювання ізраїльських політиків і військових про можливе протистояння з Іраном на технологічному фронті. Крім того, Ізраїль скорегував прогнозовану дату отримання Іраном атомної бомби, відсунувши її на 2014 рік, а повноваження Меїра Дагана, глави «Моссаду», були продовжені заради його участі у неназваних «важливих проектах». Також слід відмітити ще один цікавий факт пов'язаний із ресурсом WikiLeaks. У рамках боротьби з іранськими ядерними розробками провідні експерти з Ірану порадили уряду США віддати перевагу замість військової атаки так званому «прихованому саботажу», яким як раз і є комп'ютерний хробак Stuxnet. Про це свідчить чергова порція викриттів скандального сайту WikiLeaks, що були опубліковані британською газетою The Guardian. У статті цитується телеграма, відправлена в січні 2010 року американським послом у Німеччині Філіпом Мерфі, в якій говорилося: «берлінський Державний інститут безпеки та зовнішніх справ (Stiftung für Wissenschaft und Politik, SWP) рекомендує США застосувати саботаж, який «більш ефективний», ніж військовий удару по ядерних об'єктах.» Крім того, в цій депеші розшифровується поняття «саботаж», що включає, на думку директора SWP Фолькера Пертеса, такі інциденти як «несподівані вибухи, нещасні випадки, хакерство та ін.» Він радить надати перевагу цьому виду підривної діяльності військового удару, який призведе до руйнування всього близькосхідного регіону. Як раніше повідомляла газета The Guardian, американська адміністрація «рішуче відкинула» рекомендації Пертеса [6]. Між тим, в інтерв'ю виданню Пертеса підтвердив свою позицію, заявивши, що головна перевага такого роду дій у тому, що уряд не повинен тримати за них відповідь і буде мати можливість послатися на технічні збої.

Й справді, для передових у промисловому відношенні країн кіберзброя одночасно є і джерелом величезних можливостей, і величезною загрозою. На конференції Virus Bulletin 2010, що проходила у Ванкувері (Канада), увагу публіки привернула коротка доповідь Лаяма О Мерча одного з провідних експертів Symantec з IT–безпеки. Аналітик провів експеримент, що роз'яснив небезпеку кібер–загрози краще сотень формальних звітів. О Мерч встановив на сцені повітряний насос, що працює під управлінням операційної системи виробництва Siemens, інфікував робочу станцію, що керувала насосом, вірусом Stuxnet і запустив процес в дію. Насос швидко надув повітряну кулю, але процес не зупинився – куля надувалася до тих пір, поки не луснула. «Уявіть, що це не повітряна куля, а іранська атомна електростанція», – сказав експерт, поставивши крапку в питанні про «серйозності» кібервійни [8].

Таким чином, ряд держав заявили про необхідність формування спільної політики щодо запобігання кібератак. На даний момент не можливо точно встановити, чи призведе це до бажаного результату, навіть у тому разі, якщо буде вироблений (і підписаний) якийсь документ, що регламентує використання деструктивних технологій. Хоча й сама перспектива підписання подібного документа видається вкрай сумнівною, оскільки спокуси, пропоновані високими технологіями: анонімність, безпека (для атакуючого), безпрецедентне співвідношення «вартість / ефективність» видаються занадто привабливими. А значить, Stuxnet був лише першим прецедентом подібного масштабу на шляху техно–соціальної революції.

Щодо прогнозу на майбутній 2011 рік, то можна констатувати, що протягом останніх років фахівцям доводилося боротися з шкідливим кодом, створеним кіберзлочинцями з метою наживи. Але створення хробака Stuxnet означало, що якийсь моральний і технологічний бар'єр пройдено. Атака хробака показала всьому світу, що можливості кіберзб-

рої дуже вражаючі, а протистояння йому може виявитися вкрай складним завданням. Не виключено, що тепер програми, подібні Stuxnet, візьмуть на озброєння кіберспецслужби і комерційні компанії. Саме такі структури і стануть новими організаторами кібератак, склавши конкуренцію кіберзлочинності [9].

Зрозуміло, що за кількістю атак і вірусних інцидентів такі порушники спокою в інтернеті будуть значно поступатися традиційним кіберзлочинцям. Але при цьому їх атаки можуть бути набагато більш витонченими. Вони не будуть зачіпати звичайного користувача. Це буде невидима боротьба, епізоди якої лише зрідка випадково будуть потрапляти у поле зору ЗМІ. Більшість жертв так ніколи і не дізнається про те, як і хто завдав їм збитків. Мова йде навіть не про кібердиверсії, яким займався Stuxnet. Інформація – от що буде основною метою таких атак.

Можливо, подібні атаки тільки почнуться в 2011 році, а в повній мірі розгорнуться тільки в наступні роки. Проте вже зараз зрозуміло, що внаслідок передбачуваної появи нових атак боротьба з кіберзагрозами значно ускладниться.

Отже, підсумовуючи усе вище зазначене, можна зробити наступні прогнози, щодо основних тенденції 2011 року: у царині створення шкідливих програм та організації кібератак з'являться нові гравці. Крім отримання грошового прибутку, метою створення шкідливих програм і проведення атак стане крадіжка і подальше використання будь–якої можливої інформації. Інформація буде основною метою нових організаторів атак, і вона ж стане додатковим способом заробітку для традиційної кіберзлочинності. Традиційна кіберзлочинність буде все частіше атакувати корпоративних користувачів, поступово відмовляючись від прямих атак на домашніх користувачів. Технічні вразливості комп'ютерних систем залишаться головним шляхом здійснення атак, при цьому різноманітність використовуваних зловмисниками вразливостей і швидкість їх використання значно зростуть.

Список використаних джерел

1. Шадрин И. Червь Stuxnet разработали для глобального шпионажа [Електронний ресурс]\ И. Шадрин\\ Інтернет–портал «infox» – Режим доступу до матеріалу: http://infox.ru/hi–tech/tech/2010/09/28/stuxnetiran.phtml
2. МИД Ирана: Запуск АЭС «Бушер» задержали технические неполадки, а не вирус [Електронний ресурс]: Інтернет–портал «Росблат» – Режим доступу до матеріалу: http://www.rosbalt.ru/2010/10/05/777969.html
3. Западные СМИ: Кибероружие страшне, чем ядерное [Електронний ресурс]: Інтернет–портал «Росблат»– Режим доступу до матеріалу: http://www.rosbalt.ru/2010/10/05/777929.html
4. Гостєв А. Kaspersky Security Bulletin 2010. Развитие угроз в 2010 году [Електронний ресурс]\ А. Гостєв \\ Інтернет–портал «Securelist» – Режим доступу до матеріалу: http://www.securelist.com/ru/analysis/208050677/Kaspersky_Security_Bulletin_2010_Razvitie_ugroz_v_2010_godu#18
5. W32.Stuxnet – Network Information [Електронний ресурс]: Інтернет–портал «Symantec» – Режим доступу до матеріалу: http://www.symantec.com/connect/blogs/w32stuxnet–network–information
6. Stuxnet: война 2.0 [Електронний ресурс]: Інтернет–портал «Росблат» – Режим доступу до матеріалу: http://habrahabr.ru/blogs/infosecurity/105964/

7. Stuxnet industrial worm writtwn a year ago[Електронний ресурс]: Інтернет–портал «Security and Risk» – Режим доступу до матеріалу: http://www.csoonline.com/article/602165/stuxnet–industrial–worm–written–a–year–ago
8. О'Мерч Л. Last–minute paper: An indepth look into Stuxnet [Електронний ресурс]\ Л. О'Мерч \\ Інтернет–портал «Virus bulletin» – Режим доступу до матеріалу: http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml
9. Зайцев Ю. Кибервойна. Современные тенденции. [Електронний ресурс]\ Ю. Зайцев \\ Інтернет–портал «Security Lab» – Режим доступу до матеріалу: http://www.securitylab.ru/blog/personal/Zuis–blog/14968.php