УДК 004.49

О.В. Самчишин,
кандидат технічних наук
В.В. Охрімчук

АНАЛІЗ СУЧАСНИХ ЕЛЕМЕНТІВ КІБЕРНЕТИЧНОЇ ЗБРОЇ

У статті наведено результати аналізу сучасних елементів кібернетичної зброї. Розглянуто структуру елементів кібернетичної зброї та принцип її дії на об'єкти із критичною інфраструктурою. Встановлено взаємозв'язок між її елементами.

Ключові слова: *кіберзброя, кібератака, об'єкт з критичною інфраструктурою, взаємодія, спосіб.*

В статье приведен анализ современных элементов кибернетического оружия. Рассмотрена структура элементов кибернетического оружия и принцип его действия на объекты с критической инфраструктурой. Установлена взаимосвязь между составляющими ее элементами.

Ключевые слова: *кибероружие, кибератака, объект с критической инфраструктурой, взаимодействие, способ.*

Paper analyzes the modern elements of cyber weapons. The structure of the elements of cyber weapons and the principle of its influence on the objects with the critical infrastructure is examined. The relationship between its constituent elements is revealed.

Keywords: *cyber weapons, cyberattack, object with the critical infrastructure, interaction.*

Сучасне високотехнологічне оснащення армій розвинених країн світу дозволяє будь-якому солдату на полі бою поблизу телекомунікаційних мереж супротивника за допомогою новітньої кіберзброї запустити кібератаку та вивести з ладу об'єкт з критичною інфраструктурою. Фактично, перші зразки такої зброї є невеликими пристроями з сенсорним екраном і регулятором для збільшення або зниження інтенсивності різних видів кібератак. Розробниками кіберзброї заздалегідь вбудовується у свою продукцію достатньо великий набір різних алгоритмів з різним ступенем збитку для супротивника, а користувачеві залишається лише встановити рівень кібератаки і відстежувати її результати на сенсорному екрані. Якщо гонка кіберозброєння і надалі піде такими темпами, як нині, вже найближчим часом точки доступу Wi-Fi, ноутбуки з Wi-Fi-адаптерами та інші бездротові пристрої перетворяться на потужну сучасну зброю.

Таким чином, стає зрозуміло, що кібервійна є ефективним способом виведення з ладу будь-якого об'єкта з критичною інфраструктурою протиборчої сторони. Отже, чим більше передових інформаційних технологій перебуває у власності держави, тим більше вона уразлива для кібервторгнення іззовні. Саме тому для побудови ефективних систем кібернетичного захисту доцільно проаналізувати сучасні елементи кібернетичної зброї.

Військові експерти США вважають, що в самому лише військовому сегменті кіберпростору рівними цій державі за потужністю супротивниками є Китайська народна республіка та Російська Федерація [10, 13].

З літератури [11, 13] відомо, що китайська хакерська група NCPH створила більше 30 спеціалізованих програм, які використовують вразливості прикладних програмних засобів Microsoft Office. Як наслідок, це дозволяє впроваджувати в систему вірусні підпрограми, що дозволяють дистанційно керувати зараженими комп'ютерами, копіювати службові документи і передавати їх заданому адресату.

Відомо, що найбільш вразливими мішенями кібератак є, в першу чергу, ключові системи інформаційної інфраструктури (КСІІ), котрі керують критично важливими об'єктами. Виведення з ладу таких об'єктів може призвести до хаосу та техногенних катастроф і, як наслідок, завдати суттєвих матеріальних збитків.

Окрім промислових об'єктів, існує безліч організацій, для яких несанкціонований доступ до інформації може становити серйозну проблему. Це банки, медичні і військові установи, дослідницькі інститути, бізнес тощо. Такі організації також є мішенями для кібератак.

Таким чином, дослідження питання принципу дії сучасних елементів кібернетичної зброї, яка використовується для нападу на об'єкти з критичною інфраструктурою промислових об'єктів, є досить актуальним та перспективним напрямом досліджень, що й є метою статі.

Для управління об'єктами з критичною інфраструктурою використовується спеціалізоване програмне забезпечення, котре, як правило, має помилки та вразливості. Згідно з дослідженнями університету Карнегі-Меллона, кількість помилок у військовому та промисловому програмному забезпеченні складає в середньому від п'яти до десяти на 1000 рядків коду програми [1, 2, 5]. Так, ядро операційної системи Windows вміщає більш ніж 5 мільйонів рядків коду, а ядро Linux – не менше 3,5 мільйонів, а тому нескладно підрахувати кількість теоретично можливих вразливостей, котрі можуть застосовуватися для здійснення кібератак.

Для проведення ефективної кібератаки потрібно добре розуміти внутрішню будову об'єкта, який атакується. Саме тому алгоритм кібератаки, як правило, складається з декількох етапів.

На першому, розвідувальному, етапі збирається інформація про внутрішню будову мережі, обладнання та програмне забезпечення, що використовується. Досліджуються їх особливості та характеристики. З практики відомо, що на цьому етапі часто атакуються не цільові об'єкти, а компанії-підрядники, які здійснювали автоматизацію об'єктів, оскільки вони, як правило, менш відповідально ставляться до інформаційної безпеки. Це обумовлено тим, що такі компанії мають можливість авторизованого доступу до цільової технологічної мережі, чим зловмисники можуть скористатися на подальших етапах атаки. На стадії збору інформації можуть бути атаковані також обслуговуючі компанії, партнери, постачальники устаткування тощо.

На другому етапі зібрана інформація ретельно аналізується та обирається найбільш ефективний вектор атаки. Визначається які саме вразливості в програмному коді потрібно використовувати для проникнення в систему та яким функціоналом повинен володіти шкідливий код. Після чого створюється шкідлива програма з потрібним "боєкомплектом".

І, нарешті, на заключному етапі вирішується питання доставки шкідливого ПЗ на об'єкт. Спектр можливостей тут тягнеться від порівняно простих

методів соціальної інженерії до високотехнологічних способів проникнення через захищені канали зв'язку.

На сьогодні існує три основні види кібератак на державні інформаційні ресурси. Решта є похідними від них. Ці кібератаки спрямовані на порушення конфіденційності, цілісності та доступності інформації.

Порушення конфіденційності – це кібератаки, які спрямовані на будь-яке несанкціоноване добування інформації шляхом "аналізу мережевого трафіку".

Порушення цілісності передбачає несанкціоновану модифікацію інформації або інформаційних ресурсів.

Порушення доступності. Метою таких кібератак є створення потужних перешкод для легітимних користувачів щодо доступу їх до системи або даних, котрі їм необхідні для вирішення функціональних задач. Подібні атаки часто називають DoS та DDoS-атаками.

З розвитком інформаційних технологій та впровадженням їх у всі сфери людського життя на світову арену виходить новітній вид озброєння – кібернетична зброя, яка є засобом впливу на об'єкти критичної інфраструктури держави. Так, у період з 2009 по 2013 рік в засобах масової інформації з'являються повідомлення про вплив на об'єкти критичної інфраструктури країн Близького Сходу такими шкідливими програмами, як Stuxnet, Duqu, Flame та Gauss, котрі спеціалісти у сфері інформаційних технологій провідних країн світу відносять до кібернетичної зброї [2, 9, 11, 13]. Розглянемо детальніше принцип дії цієї кібернетичної зброї.

Вперше комп'ютерний вірус Stuxnet був виявлений в червні 2009 року білоруською компанією Virusblokada, котра спеціалізується на комп'ютерній безпеці, в одному з комп'ютерів іранського клієнта. Цей зразок кібернетичної зброї використовує декілька вразливих ланок в системі Windows. Серед них – LNK/PIF Files Automatic Execution, Windows Print Spooler Service Remote Code, через SMB за допомогою вразливості Server Service RPC.

Потрапляючи до корпоративної мережі через заражений USB-пристрій, кібернетична зброя Stuxnet використовує ті помилки, котрі підвищують його привілеї (EoP) в мережі з метою одержання несанкціонованого доступу на правах адміністратора. Далі розшукуються ті системи, в яких працюють програми керування WinCC та PCS 7 SCADA компанії Siemens. Ці системи використовуються у всьому світі для керування виробничим устаткуванням. Саме ця система використовувалася для контролю устаткування для збагачення урану в Ірані. Кібернетична зброя вражає контролерів частоти напруги, що подається на електромотори. Особливістю кібернетичної зброї Stuxnet є те, що вона вражає тільки тих контролерів, які поставлялися іранською компанією Fararo Paya або фінською компанією Vacon. Саме ці контролери були встановлені на іранських уранозбагачувальних комбінатах в Бушері та Натанзі. Кіберентична зброя Stuxnet захоплювала ці системи, використовуючи помилку спулера друку, потім намагалася застосувати фабричний пароль Siemens для захоплення керування програмним забезпеченням SCADA. Після чого Stuxnet перепрограмовував програму PLC (programmable logic control – програмований логічний контролер), щоб керувати всіма механізмами, які керуються цією системою. Таким чином, нормальні режими роботи системи на частоті в 600 Гц були спочатку змінені на 1410 Гц, потім – на 2 Гц, а в кінцевому рахунку – на 1064 Гц. Причому такі зміни тривали періодичний, але короткотривалий хпрактер.

Другою особливістю кібернетичної зброї Stuxnet є мінімізація атакуючою стороною ризиків виявлення присутності своєї програми. У кожному USB-пристрої, які були заражені вірусом Stuxnet, працював лічильник, який контролював кількість заражених пристроєм комп'ютерів та не дозволяв інфікувати більш ніж три комп'ютери. Таким чином, суб'єкт атаки штучно обмежував масштаб розповсюдження кібернетичної зброї.

Функціонування кібернетичної зброї Stuxnet розраховано на повністю автономну роботу програми й не вимагає підключення до мережі Інтернет з метою одержання додаткових інструкцій та управління з боку людини взагалі. Умовна схема архітектури платформи Stuxnet за даними [6] має вигляд як на рис. 1.

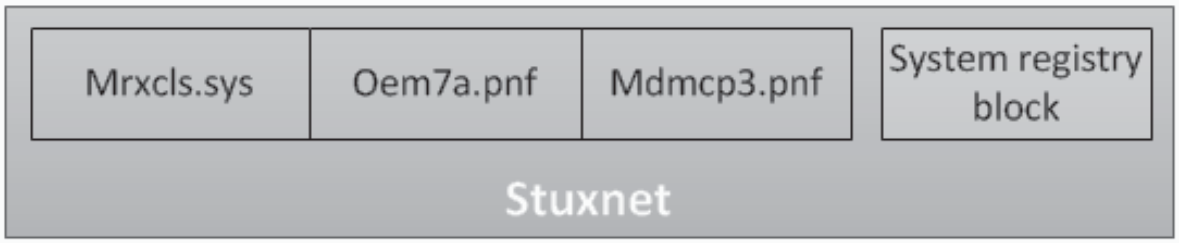

Рис. 1. Умовна схема архітектури платформи кібернетичної зброї Stuxnet

За час свого існування вірус заразив приблизно 100 тисяч хостів. З них більш ніж 60 тисяч в Ірані, близько 13 тисяч в Індонезії та приблизно 7 тисяч в Індії. Також було відзначено зменшення числа активних центрифуг, що збагачували уран в Ірані, з 4700 до 3900, що також було пов'язано з роботою віруса Stuxnet [6, 8, 9].

Таким чином, у результаті аналізу встановлено, що Stuxnet – це високоточна, суто вибіркова кібернетична зброя, метою якої є пошук та знищення однієї єдиної конкретної цілі.

Іншим зразком кібернетичної зброї, що підлягає аналізу, є троянська програма Duqu, програмний код якої схожий з кібернетичною зброєю Stuxnet. На відміну від Stuxnet, Duqu розроблений для крадіжки конфіденційної інформації з комп'ютерів користувачів [2, 6]. Умовна схема архітектури платформи Duqu за даними може бути зображена на рис. 2 [6].

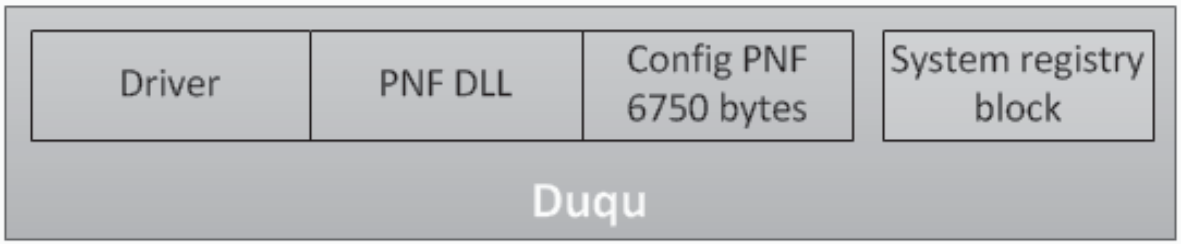

Рис. 2. Умовна схема архітектури платформи кібернетичної зброї Duqu

Суттєвою відмінністю кібернетичної Stuxnet від Duqu є те, що останній зразок є розвідником, котрий збирає інформацію для підготовки наступного удару, а потім приховує сліди своєї присутності. Згідно з [6], відомо, що через 36 днів після зараження кібернетична зброя Duqu самоліквідовується.

У травні 2012 року спеціалістами "Лабораторії Касперського" була виявлена кібернетична зброя Flame, основним завданням якої був кібершпіонаж. Flame є досить різноманітний набір інструментів для проведення кібератак, який значно перевищує за складністю Duqu. [7] Це троянська програма – бекдор, яка має також характерні риси притаманні комп'ютерним "черв'якам". Така особливість дає їй можливість розповсюджуватись локальною мережею та через USB носії.

Після зараження системи Flame розпочинає виконання складного набору операцій, в тому числі аналіз мережного трафіку, створення знімків екрану, аудіозапису розмов, перехоплення клавіатурних натискань тощо. Усі ці дані доступні операторам через командні сервери Flame. У майбутньому оператори можуть приймати рішення про завантаження на заражені комп'ютери додаткових модулів, що розширюють функціонал Flame. Усього згідно з [7,13] існує близько 20 модулів, призначення більшості яких на цей момент досліджується фахівцями. Перш за все, Flame – це пакет програмних модулів, загальний розмір яких при повному розгортанні складає не менше 20 Мб. Саме тому ця шкідлива програма досить складна для аналізу. Причиною такого великого розміру Flame є те, що до її складу входить велика кількість бібліотек, у тому числі для стискання коду (zlib, libbz2, ppmd) та маніпуляції базами даних (sqlite3), а також віртуальна машина Lua.

Існує цілий ряд характерних ознак, які відрізняють кібернетичну зброю Flame від інших шкідливих програм та роблять її унікальною [7, 11, 13]. Перш за все, для шкідливого програмного забезпечення є нехарактерним використання Lua. Досить великий розмір набору інструментів для проведення атак також є нетиповим для шкідливого ПЗ. Як правило, сучасні шкідливі програми мають невеликий розмір та пишуться на мовах програмування, котрі забезпечують максимальну компактність, що дозволяє приховати ці програми в системі. Приховування за допомогою великого об'єму коду – це нова ознака, котра реалізована у Flame. Запис аудіоданих із вбудованого мікрофона – також досить новий прийом. Ще одна суттєва ознака Flame – використання Bluetooth у пристроях, що підтримують такий спосіб передачі даних. Якщо Bluetooth підтримується зараженим комп'ютером та ввімкнений у налаштуваннях, програма збирає інформацію про виявлені пристрої, що оточують заражену машину. Якщо в конфігурації ввімкнені відповідні налаштування, Flame може перетворити заражену машину на радіомаяк, налаштувавши дозвіл на його виявлення іншими Bluetooth-пристроями.

За період з 2010 року й до сьогодні було виявлено біля 200 заражених систем, які знаходяться в Ірані, близько 100 в Ізраїлі та Палестині, приблизно по 30 систем в Сирії та Судані, решта розміщуються в Саудівській Аравії, Єгипті, Лівані та інших державах цього регіону. IP-адреси серверів, що керують кібератакою Flame, постійно підміняються PROXY-серверами, запобігаючи, таким чином, виявленню місця походження кібернетичної зброї. На сьогодні нараховується близько 80 IP-адрес серверів, що керують атакою Flame.

Майже одночасно з виявленням Flame була виявлена ще одна складна шкідлива програма, котру експерти також віднесли до класу кібернетичної зброї. Шкідлива програма була створена в середині 2011 року та вперше застосована в серпні – вересні того ж року. Ця програма була названа на честь німецького математика Йоганна Карла Фрідріха Гаусса [12].

Gauss – банківська троянська програма, реалізована тією ж групою, що створила Flame. Gauss має шкідливий функціонал невідомого й досі призначення.

Кібернетична зброя Gauss – це складний комплекс інструментів для проведення кібершпіонажу. Комплекс має модульну структуру та підтримує віддалене розгортання операторами нового функціоналу, котрий реалізується у вигляді додаткових модулів Відомі на сьогодні модулі виконують такі функції: перехоплення cookie-файлів та паролів у браузері; збір та відправка зловмисникам даних про конфігурацію системи; зараження USB-носіїв модулем, призначеним для крадіжки даних; створення списків з вмістом системних накопичувачів та папок; крадіжка даних, необхідних для доступу до облікових записів різних банківських систем, що діють на Близькому Сході; перехоплення даних за обліковими записами в соціальних мережах, поштових сервісах та системах миттєвого обміну повідомленнями.

Модулі, що реалізують описані вище функції, названі на честь відомих математиків та філософів, таких як Курт Гйодель, Йоганн Карл Фрідріх Гаусс та Жозеф Луї Лагранж.

Модуль під назвою Gauss – найбільш важливий елемент шкідливої програми, оскільки в ньому реалізовані можливості, пов'язані з крадіжкою банківських даних. Саме тому весь шкідливий комплекс бав названий ім'ям цього модуля. На рис. 3 представлена архітектура кібернетичної зброї Gauss [12].

Порядок зараження об'єктів із критичною інфраструктурою кібернетичною зброєю Gauss до сьогодні також не встановлено. При цьому не виключається, що Gauss використовує ті ж механізми зараження, що і Flame. Під час дослідження Gauss не було виявлено механізму саморозповсюдження (як у комп'ютерних черв'яків), однак велика кількість жертв може вказувати на наявність цієї функції. Можливо, ця функція реалізована в модулі, котрий досі є невідомим.

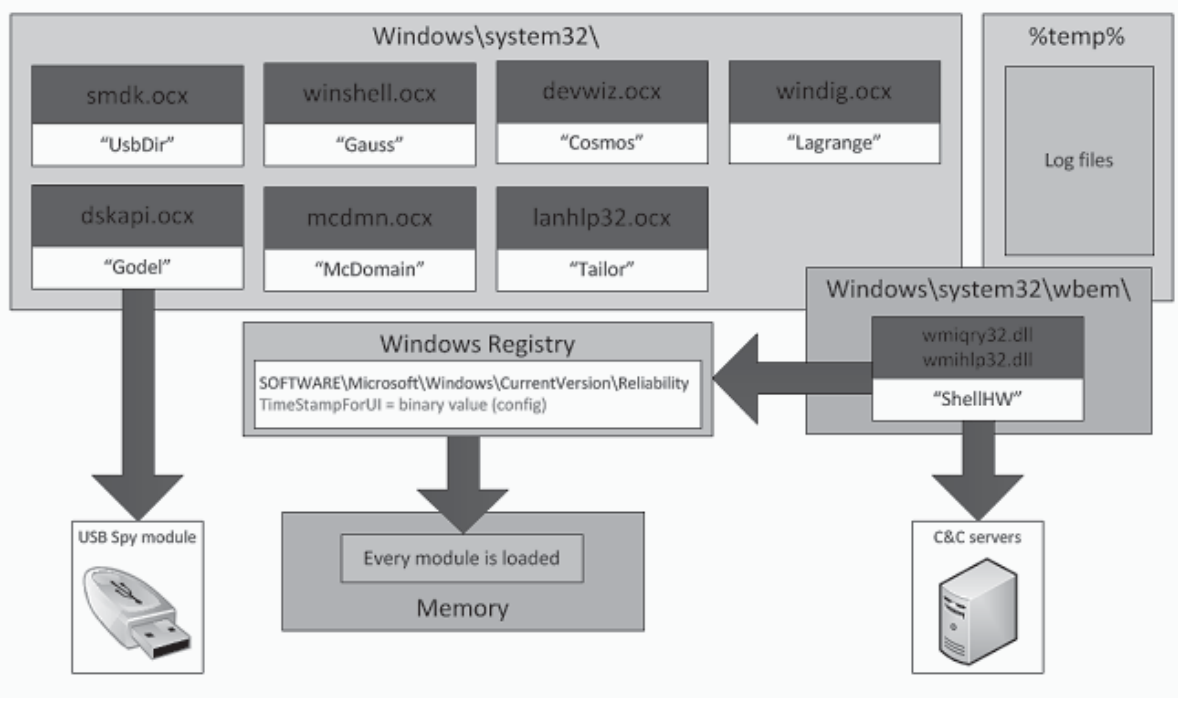

Рис. 3. Архітектура Gauss

Важливою рисою Gauss є те, що він заражає USB-носії компонентом, призначеним для крадіжки даних, що використовує ту ж вразливість LNK (CVE-2010-2568), яку експлуатують Stuxnet та Flame. Водночас має місце більш інтелектуальний та ефективний процес зараження USB-носіїв. Gauss спроможний до "знезаражування" носів за певних обставин. Слід зазначити, що схожою властивістю до збереження інформації в прихованому файлі на USB-носії володіє також кібернетична зброя Flame.

Після аналізу таких елементів кібернетичної зброї, як Stuxnet, Duqu та Flame можна зробити висновок, що розробником кібернетичної Gauss є ті самі держави, а тому взаємозв'язок цих зразків можна подати у вигляді рис. 4.

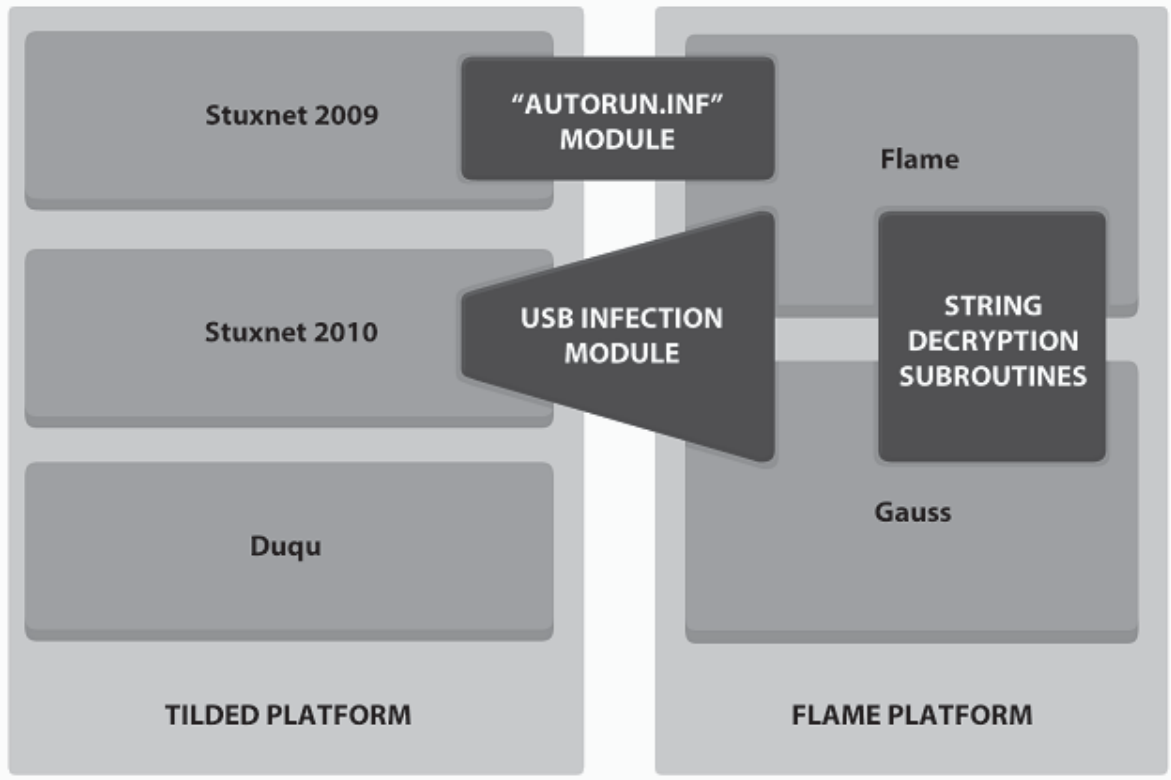

Рис. 4. Взаємозв'язок між елементами кібернетичної зброї Flame, Gauss, Stuxnet та Duqu

Попри те, що Gauss і Flame мають багато спільного в архітектурі побудови, їх географія зараження суттєво різниться. Максимальна кількість комп'ютерів, уражених Flame, припадає на Іран, тоді як більшість жертв Gauss знаходяться в Лівані. Кількість заражених комп'ютерів також різниться. За даними системи моніторингу Kaspersky Security Network, Gauss заразив близько 2,5 тисяч комп'ютерів, тоді як жертв Flame було всього біля 700 [12].

Таким чином, проаналізувавши елементи кібернетичної зброї, можна зробити висновок, що провідні країни світу готуються до ведення кібервійни. В обов'язковому порядку ними розробляються як наступальні операції, так і оборонні елементи кібернетичної зброї. Тому цілком очевидно, що нині вкрай необхідно проводити якісну підготовку висококваліфікованих фахівців з питання кібербезпеки, у тому числі за рахунок ґрунтовного вивчення принципів дії та структури елементів кібернетичної зброї.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методы и средства защиты информации : в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко ; под ред. В.А. Хорошко. – К. : Арий, 2008 – Т. II. Информационная безопасность. – 344 с.

2. *Грищук Р.В.* Атаки на інформацію в інформаційно-комунікаційних системах / Р.В. Грищук // Сучасна спеціальна техніка. – 2011. – № 1(24). – С. 61–66.

3. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М. : ДМК Пресс, 2010. – 544 с.

4. *Лукацкий А.В.* Обнаружение атак / А.В. Лукацкий – С-Петербург : БХВ-Петербург, 2003. – 256 с.

5. *Лукацкий А.В.* Предотвращение сетевых атак : технологии и решения / А.В. Лукацкий. – С-Петербург : Экспресс Электроника, 2006. – 268 с

6. Stuxnet/Duqu : The Evolution of Drivers [Электронный ресурс]. – Режим доступа : http : // securelist.com/analysis/publications/36462/stuxnetduqu-the-evolution-of-drivers/.

7. The Flame : Questions and Answers [Электронный ресурс]. – Режим доступа : http : // securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/#page_top.

8. Безопасность SCADA : Stuxnet – что это такое и как с ним бороться? [Электронный ресурс]. – Режим доступа : http : // www.securitylab.ru/analytics/400024.php.

9. Stuxnet и промышленная безопасность [Электронный ресурс]. – Режим доступа : http : // www.phocus-scada.com/rus/pub/Stuxnet&IndustrialSecurity.html.

10. Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств [Электронный ресурс]. – Режим доступа : www.securitylab.ru/analytics/398184.php.

11. Американские военные испытывают оружие для ведения кибератак [Электронный ресурс]. – Режим доступа : www.securitylab.ru/news/380170.php.

12. Gauss : государственный кибершпионаж плюс [Электронный ресурс]. – Режим доступа : http : // securelist.ru/blog/spam-test/2930/gauss-gosudarstvennyj-kibershpionazh-plyus/.

13. Кибервойна. Современные тенденции / Security Lab [Электронный ресурс]. – Режим доступа : www.securitylab.ru/blog/personal/Zuis-blog.

Отримано 12.09.2014

Рецензент Яковенко О.В., старший науковий співробітник, професор.