ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 354.42/44:343.9

До питання протидії використанню шкідливого програмного забезпечення

Гавловський Владислав Данилович –
начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат юридичних наук, старший науковий співробітник

На підставі проведеного аналізу, в контексті проблем захисту національної безпеки України в інформаційній сфері, наводиться аргументація щодо необхідності розробки та реалізації комплексу організаційно-практичних заходів протидії протиправному використанню шкідливого програмного забезпечення, а також розробки національного антивірусного програмного забезпечення.

Ключові слова: шкідливе програмне забезпечення, програми-шпигуни, інформаційна безпека, антивірусне програмне забезпечення.

Постановка проблеми. Впровадження нових інформаційних технологій призвело до формування єдиного світового інформаційного простору, де кожен користувач має можливість отримати доступ до, фактично, будь-якої інформації, потрібної йому, незалежно від державних чи географічних кордонів.

Однак, величезні можливості сучасних інформаційних мереж, усе більше і більше, використовуються із протиправною, зокрема, злочинною метою як представниками організованих злочинних угруповань, так і особами, зацікавленими у різноманітній деструктивній діяльності. Вочевидь, що на сьогодні, через відсутність державних кордонів, кіберпростір перетворився на, майже ідеальне місце вчинення злочину, а інформаційні ресурси все частіше використовуються як засіб чи знаряддя вчинення злочину, перетворюючи конкретну інформацію на предмет злочину. Відтепер для вчинення злочину не потрібно навіть особистого контакту з потенційною жертвою. Головним інструментом злочинця стає лише комп'ютер і його фактичний доступ до інформаційно-комунікаційних систем, де за допомогою шкідливих програмних та інших протизаконних технічних засобів можливо отримати доступ до персоніфікованих баз даних, банківських рахунків, автоматизованих систем управління тощо.

Зокрема, у доповіді Європолу про стан злочинності в ЄС та нових явищах і тенденціях у кримінальній сфері, що ґрунтується на плані дій Європарламенту на 2014–2019 рр. щодо боротьби з новими видами злочинності, відмиванням грошей та корупцією, зазначено, що процес інфікування комп'ютерно-телекомунікаційних пристроїв потенційних жертв шкідливим програмним забезпеченням – ключовий компонент цифрової підпільної економіки. Згідно з дослідженням Europe-based security company, близько 38 % комп'ютерних систем і пристроїв у країнах ЄС є інфікованими [1].

Показовим, з точки зору небезпечності вказаного явища, є те, що лише шкідливим програмним забезпеченням "Gameover Zeus", яке зловмисники використовували протягом тривалого часу для здійснення атак на сайти провідних фінансових установ світу, були інфіковані близько мільйона комп'ютерів по всьому світу, в тому числі понад 60 тис. на території України, при цьому, збитки від протиправної діяльності оцінюються фахівцями у 75 млн євро [2].

При цьому, останнім часом розповсюдження шкідливого програмного забезпечення стало набувати все більш загрозливіших масштабів. І, незважаючи на величезні зусилля конкуруючих між собою антивірусних фірм-виробників антивірусних засобів, збитки, завдані шкідливим програм-

ним забезпеченням, збільшуються та сягають сотень мільйонів доларів США щорічно.

Одночасно варто враховувати, що таке шкідливе програмне забезпечення було і залишається однією з найбільш поширених причин витоку та незворотної втрати важливої для фінансової, економічної, наукової та військової сфери держави інформації. До того ж такі шкідливі програми постійно вдосконалюються фахівцями, які знаходять усе нові, більш витончені способи несанкціонованого проникнення до комп'ютерів користувачів та інформаційних систем.

Так, наприклад, аналізуючи шкідливу програму, якій надали умовну назву "Челябінськ", фахівці компанії "Лабораторія Касперського" зазначають, що за своєю складністю вона значно перевищує не тільки існуючі нині шкідливі програми, включаючи професійні шпигунські кібератаки і кіберзброю, але й будь-яке інше відоме програмне забезпечення [3].

Показовим є звіт компанії Panda Security за I квартал 2014 р., в якому зазначається, що вже за три перших місяці поточного року було створено більше 15 млн нових шкідливих програм, тобто, щодня їх кількість збільшується на 160 тис. [4].

У той же час, варто звернути увагу на те, що окремою та, без перебільшення, найнебезпечнішою з точки зору державної, економічної та інформаційної безпеки України сьогодні є така категорія шкідливого програмного забезпечення, як програми-шпигуни. У цьому контексті варто звернути увагу на відсутність у нашій державі належного рівня національного антивірусного програмного забезпечення. Вочевидь, що антивірусні програмні продукти, що розроблені іноземними кібер-компаніями, не можуть, з одного боку, врахувати на достатньому рівні конкретні потреби захисту національної складової інформаційного простору, що включає і закриту, таку, що належить виключно державі або охороняється нею, конфіденційну інформацію, потрапляння якої до іноземних розробників антивірусних програм є неприпустимим, через фактичну шкоду навіть від цього національній безпеці України, а, з іншого, через неможливість гарантування того, що представники іноземних спецслужб не використовують антивірусні програми національних розробників для того, щоб блокувати виявлення власних програм-шпигунів. Як бачимо, і в останньому випадку використання іноземного антивірусного програмного забезпечення, також є небажаним з точки зору забезпечення національної безпеки України.

Отже, тут єдиним прийнятним виходом є розробка національного антивірусного програмного забезпечення. Варто з позитивного боку відзначити позицію керівництва нашої держави, що своєчасно та адекватно відреагувавши на викликані вищезазначеними загрозами національній безпеці Україні потреби, в Указі Президента України № 449/2014 "Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" прямо передбачило опрацювання питань створення національного антивірусного програмного забезпечення [5]. Отже, тематика, обрана для представленого дослідження, є важливою та **відповідає критерію актуальності**.

Метою представленої праці є аналіз, у контексті національної безпеки України в інформаційній сфері, виявлених іноземними фахівцями в останні роки програм-шпигунів, надання аргументації щодо розробки та реалізації комплексу організаційно-практичних заходів щодо протидії протиправному використанню шкідливого програмного забезпечення в нашій державі та розробки національного антивірусного програмного забезпечення.

Аналіз останніх досліджень і публікацій. Дослідженням проблемних питань, пов'язаних зі здійсненням організаційно-правових та організаційно-практичних заходів протидії злочинній діяльності у кіберпросторі, в контексті забезпечення національної безпеки України, займалися такі провідні вітчизняні вчені, як В. М. Бутузов, О. Ф. Гіда, О. В. Копан, А. І. Марущак , В. Г. Пилипчук, В. П. Шеломенцев, О. М. Юрченко та інші. У той же час, дослідження конкретних проблемних організаційно-практичних питань щодо протидії використанню у контексті інформаційних ресурсів нашої держави програм-шпигунів і створення національного антивірусного забезпечення досі є недостатньо дослідженим. У цьому контексті представлена праця є логічним продовженням раніше розпочатого та здійснюваного нами дослідження [6], що і зумовлює **відповідність даної праці критерію наукової новизни.**

Виклад основних положень. Програми-шпигуни – це шкідливі програмні засоби, які після їх проникнення до певної АС, комп'ютерної мережі, операційної системи ЕОМ чи окремої комп'ютерної програми забезпечують несанкціонований доступ сторонньої особи до інформації, яка зберігається у ЕОМ, АС, мережі чи програмі або ж непомітно для власника чи законного користувача здійснюють несанкціоновану передачу такої інформації сторонній особі [7].

Вони найчастіше використовуються з метою незаконного збору розвідувальних даних спецслужбами різних держав – надають можливість отримувати доступ до конфіденційної інформації, в тому числі й персональної. Останнім часом виявляються програми, які на протязі кількох років незаконно збирали різну інформацію з комп'ютерів урядових, дипломатичних, військових та наукових установ і організацій, а також окремих об'єктів критичної інфраструктури на території різних країн світу.

Так, на початку минулого року фахівці "Лабораторії Касперського" виявили шкідливу програму, якій дали назву Red October. Вона функціонувала з 2007 року. Для зараження систем використовувалися фішингові листи, які мали конкретних адресатів, відповідно до їхніх індивідуальних особливостей, що свідчить про

попереднє вивчення інформації щодо потенційної жертви [8].

Крім цього, у 2013 році було виявлено ще дві програми-шпигуни. Одну з них – MiniDuke – було виявлено спільними зусиллями "Лабораторії Касперського" та угорською компанією Cry-Sys Lab (Лабораторія криптографії і системної безпеки). Серед жертв цього вірусу нараховується 59 державних установ із 23 країн світу, в тому числі й України. Вона проникала на комп'ютери користувачів через прогалини в додатках Adobe Reader з використанням PDF-файлів, які, до речі, досить ретельно підбиралися і були надзвичайно актуальними для потенційних жертв. Так, у них містилася інформація, яка стосувалась семінарів про права людини (ASEM), даних про зовнішню політику України, планів держав-учасниць НАТО [9].

На початку червня 2013 року "Лабораторія Касперського" розкрила ще одну програму-шпигуна NetTraveler. В її рамках цільовим атакам піддалися більше 350 комп'ютерних систем із 40 країн світу. До числа потерпілих увійшли державні організації, посольства, компанії з нафтовидобувної та газової промисловості, дослідницькі центри, військові структури та громадські активісти [10].

Вже цього року "Лабораторія Касперского" оголосила про виявлення глобальної програми-шпигуна "Маска", за якою стоять іспаномовні зловмисники. Дії зловмисників, у першу чергу, були спрямовані на державні організації, дипломатичні представництва і посольства, енергетичні й нафтогазові компанії, дослідницькі організації і політичних активістів. Жертвами цієї таргетованої атаки стали 380 користувачів із 31 країни, включаючи Близький Схід, Європу, Африку та Америку.

За оцінками експертів, розмір і складність структури шкідливих порграм, рівень організації самої діяльності з відслідковування свідчать про причетність до реалізації цієї програми спеціальних служб, оскільки спостерігається вкрай високий рівень професіоналізму в діях групи, яка забезпечує моніторинг власної інфраструктури, приховує себе, а також, за необхідності, припиняє будь-які дії.

Дослідження показало, що операція "Маска" активно велася впродовж 5 років до січня 2014 року.

Зараження комп'ютерів користувачів відбувалося через розсилку фішингових листів, що утримують посилання на шкідливих ресурсах. У разі успішної спроби зараження, шкідливий сайт перенаправляв користувача на нешкідливий ресурс, який згадувався в листі, це міг бути YouTube або новинний портал [11].

Зазвичай, коли з'являється інформація про нову великомасштабну атаку, що націлена на технологічну компанію, державну організацію або фінансову установу – вся увага зазвичай концентрується на жертвах і на предметі злочинної діяльності. Однак, виявлені атаки можуть бути лише окремими епізодами довготривалої серії операцій.

Так, під час однієї з них, що дістала назву Icefog ("Крижаний Туман"), зловмисники атакували організації та установи найширшого спектру галузей в декількох країнах, переважно в Японії і Кореї. Серед потерпілих – постачальники американських оборонних підрядників, наприклад, Lig Nex1, яка виготовляє дисплеї для американських літаків F15, кораблебудівні компанії, телекомоператори і медійні компанії. Тобто самі підходи до вибору жертв і манера дій зловмисників свідчать, що вони є найманцями і намагаються отримати інформацію, яка цікавить їхніх замовників. Зазвичай, організатори Icefog, як тільки отримують необхідну для замовника інформацію, залишають ресурси жертви, видаляючи усі сліди свого перебування [12].

У травні 2012 року фахівці "Лабораторії Касперського", на прохання Міжнародного союзу електрозв'язку, вивчали версію про можливу шкідливу програму на комп'ютерах у Міністерстві нафти і газу Ірану. Так, було виявлено програму Flame. У червні американська преса вперше підтвердила, що Stuxnet і Flame були зброєю тіньової війни США та Ізраїлю з Іраном.

Нещодавно фахівцями німецької компанії-виробника програмного забезпечення, що спеціалізується на IT-безпеці, G Data Software AG було виявлено нову шкідливу програму – руткит Uroburos, яка діє з 2011 року й призначена для викрадення конфіденційної інформації з комп'ютерних систем державних установ, спецслужб і великих компаній. Фахівці зазначеної компанії стверджують, що структура і сучасний дизайн руткита Uroburos дуже складні, надзвичайно гнучкі та небезпечні, а його створення вимагає великих інвестицій. Комплексна структура драйвера цього шкідливого програмного забезпечення спроектована так, що виявити його дуже складно [13].

Через деякий час британський оборонний підрядник BAE Systems Applied Intelligence повідомив про виявлення нового шкідливого програмного забезпечення, що атакує урядові установи Великобританії. У термінології BAE цей код, який характеризується надзвичайно високою складністю, отримав назву "Snake".

Його присутність було зафіксовано фахівцями компанії Blue Bridge Baltic (Литва) на державних сайтах України ще до початку політичної кризи. Причому атаки здійснювалися в найважливіші для країни моменти [14].

Фахівцями антивірусної компанії Symantec також було виявлено шкідливе програмне забезпечення, яке заражало урядові мережі по всьому світу й якому привласнили назву Turla. Експерти цієї компанії говорять, що жертвами Turla стали вже близько 1000 мереж. Крім цього, технічний директор Symantec Security Response Е. Чен, відмітив, що Turla – це "подальша еволюція" Agent.BTZ. Цю думку підтвердили також і у фінській корпорації Інтернет-безпеки F-Sekure, стверджуючи, що Turla і Agent.BTZ є шкідливими програмами одного сімейства.

Слід також відмітити, що у 2008 році шкідлива програма Agent.BTZ вразила локальні мережі Центрального командування Збройних Сил США на Близькому Сході. Ця атака була визнана найбільшою атакою в комп'ютерній історії Збройних Сил США, на ліквідацію наслідків якої Пентагон витратив майже 14 місяців. Шкідлива програма здійснювала пошук і відправку цінної інформації із заражених комп'ютерів у віддалений центр управління. Цей випадок став каталізатором для створення нового підрозділу Збройних Сил США – Кібернетичного командування [15].

Зазначимо, що експерти вважають, що Turla, Uroburos та Snake – це одна і та ж сама шкідлива програма.

В результаті вивчення вказаного шкідливого програмного забезпечення фахівці встановили, що тактика здійснення атак обирається диференційовано для кожної окремої жертви, а не атакують максимально широко, сподіваючись хоча б раз потрапити в ціль, як це роблять китайські проурядові хакери.

За твердженням західних експертів, розробкою руткита займалися представники спецслужб Росії, про що свідчить тактика, за якою діють хакери, а також безліч технічних індикаторів і жертви, які були атаковані. Разом з тим, фахівці з безпеки попереджають: зв'язок з Росією – це лише здогадка, яку неможливо підтвердити доти, поки спецслужби Росії самі не візьмуть на себе відповідальність за створення вірусу, оскільки розробники цього руткита використовують технології для приховування особистості. ФСБ від коментарів відмовилася. А фахівці "Лабораторії Касперського" заперечують причетність російських спецслужб до розробки руткита і Agent.BTZ, а також прямий зв'язок між групами зловмисників, які їх розробляли [16].

Зазначимо, що в компанії "Лабораторії Касперського" працюють більше 2800 висококваліфікованих фахівців. Вона є одним із провідних світових виробників програмного забезпечення для антивірусного захисту (Endpoint Protection). Продукти і технології компанії використовуються більш ніж 300 млн індивідуальних користувачів і більше 250 тис. корпоративних клієнтів у світі. До того ж, "Лабораторія Касперського" вважається лідером з виявлення програм-шпигунів.

З 8 серпня 2007 року Генеральним директором компанії є її засновник – Є. Касперський, який служив у радянській розвідці, а нині знаходиться в альянсі з режимом Путіна, співпрацює з ФСБ. "Лабораторію Касперського" називають фактичним підрозділом ФСБ. Хоча сам Касперський такий зв'язок очолюваної ним компанії з ФСБ РФ заперечує.

Відносини Кремля і "Лабораторії Касперського" багато в чому схожі на відносини Вашингтона з великими американськими антивірусними компаніями : робота за держзамовленнями, розшук кіберзлочинців і проведення брифінгів для законодавців.

Але існують і суттєві відмінності. Наприклад, Stuxnet була суворо засекреченою операцією уряду США, але американська компанія Symantec все одно зайнялася боротьбою з цим вірусом [17].

Також слід нагадати, що напередодні виборів в Україні зловмисниками було зламано виборчу систему ЦВК і тимчасово виведено з ладу IT-інфраструктуру Центрвиборчкому. При цьому встановлений на комп'ютері адміністратора ЦВК антивірус "Касперського" не спрацював.

Тому, виходячи із вищесказаного і реалій сьогодення, необхідно провести експертизу антивірусних продуктів компанії "Лабораторія Касперського" з метою визначення потенційних загроз для органів державної влади України.

Крім цього, Україні конче необхідно мати своє потужне національне українське антивірусне програмне забезпечення. Тим більше, що є певний досвід розробки таких програм.

Першу вітчизняну антивірусну комп'ютерну програму (УНА/UNA) було створено на початку століття. В 2005 році фахівці зазначали, що її український варіант за своїми технічними можливостями перевершував відомі закордонні аналоги. Тоді користувачами УНА були : державні (63 %) та комерційні (22 %) організації, приватні особи (8 %), навчальні заклади (7 %). Серед них, зокрема: Кабінет Міністрів України, Секретаріат Президента України, Національний банк України, Державна податкова служба України, "Енергоатом", "Дніпроспецсталь", ТНК "Україна", "Альфа-Банк" тощо. Проте, у квітні 2007 року підтримку і фінансування цього продукту було призупинено [18].

Наступною спробою забезпечити державу власним програмним антивірусним захистом було створення в 2009 році фахівцями з IT-безпеки антивірусу Zillya. Незважаючи на те, що, за оцінками експертів, ця розробка є достатньо посередньою, все ж вона здатна забезпечити певний рівень захисту ПК від уже відомих загроз.

Під час чергового щоквартального тестування (I On-Demand), організованого у січні 2014 року порталом SAFETY-GATE.RU, де перевірялась ефективність 38 антивірусних програмних продуктів, антивірус Zillya з детектом 52,64 % посів 35 позицію. Перше місце в цьому рейтингу дісталось антивірусній програмі Trust-Port Total Protection з рівнем детекта 99,09 %, а антивірус компанії Kaspersky Internet Security з детектом 90,53 % посів 23 позицію. Таким чином, робота над удосконаленням власної системи антивірусного програмного забезпечення та її впровадженням для захисту національних комп'ютерних мереж є цілком реальним завданням, реалізація якого сприятиме зміцненню інформаційної безпеки держави [19].

Необхідно звернути увагу ще на один аспект забезпечення інформаційної безпеки держави. Він стосується формування достатнього потенціалу фахівців у цій сфері професійної діяльності.

За даними Асоціації інформаційних технологій України, сьогодні в країні загалом працює

близько 200 тис. ІТ-спеціалістів. З них : у м. Києві – 17,5 тис., м. Харкові – 5,5 тис., м. Львові – 4,6 тис., м. Дніпропетровську – 4 тис.

Крім цього, вищими навчальними закладами України щорічно готується близько 15 тис. фахівців цього профілю. У той же час, відсутність державного замовлення на таку кількість спеціалістів та їх низька заробітна платня в державному секторі призвели до загострення проблеми відтоку висококваліфікованих фахівців у сфері інформаційних технологій як за кордон, так і в "тіньовий" сектор національної економіки чи аутосорсингові компанії [20].

Зниження офіційного попиту на дипломованих ІТ-фахівців в Україні призвело до збільшення їх кількості на обліку в центрах зайнятості, через які працевлаштовується, як правило, лише кожний третій. У той же час, попит на таких фахівців у світі зростає. Це призвело до збільшення випадків їх працевлаштування в іноземних компаніях, де наші фахівці вважаються достатньо кваліфікованою і відносно дешевою робочою силою. Так, лише з числа випускників факультету кібернетики Київського національного університету ім. Тараса Шевченка кожного року виїжджає за кордон на роботу за спеціальністю близько 20 % найбільш підготовлених і обдарованих молодих фахівців.

До-речі, студенти факультету кібернетики постійно беруть участь у різних конкурсах і чемпіонатах як європейських, так і світових. Починаючи з 2006 року, вони майже постійно є серед призерів. Так, на чемпіонаті 2009/2010 років у м. Харбіні (Китай) вони зайняли 4 місце, на чемпіонаті 2012/2013 років у м. Санкт-Петербурзі (Росія) – 7 місце.

Слід також мати на увазі, що великі транснаціональні компанії, такі як Microsoft, Google, Facebook, "полюють" на українських комп'ютерних геніїв. Для цього ними організовуються різні чемпіонати світу з програмування, після яких пропонується працевлаштування. Як приклад, у поточному році 15 студентів факультету кібернетики, пройшовши конкурсний відбір, в якому брали участь студенти з усього світу, отримали можливість пройти стажування в компанії Facebook. Зазначимо, що конкурс складав 150 кандидатів на одне місце [21].

Серед шляхів вирішення зазначених проблем є посилення державної підтримки розвитку індустрії програмної продукції, зокрема, через створення технополісів, як одного з елементів інноваційної інфраструктури. Їх розвиток у всьому світі свідчить про ефективність втіленого у них підходу до забезпечення перетворення нових ідей в унікальну науково-технічну продукцію завдяки поєднанню на певній території всіх елементів національної інноваційної системи. Технопарки сприяють навчальним і науковим організаціям у впровадженні новітніх технологій в економіку, створенні нових видів виробництв і нових робочих місць. Сьогодні програми будівництва технополісів реалізуються в Китаї, Таїланді, Індонезії, Філіппінах, Малайзії. У технічні мегаполіси перетворюються Японія та Австралія. На жаль, така робота майже не проводиться в Україні.

Головні висновки роботи:

1. Проблема протидії розповсюдженню та використанню щодо інформаційних ресурсів нашої держави програм-шпигунів є, на сьогодні, важливою для забезпечення інформаційної безпеки України – складової національної безпеки та потребує підвищеної уваги з боку державних органів що діють у цій сфері.

2. В умовах сьогодення необхідним для забезпечення інформаційної безпеки України є створення саме національного антивірусного програмного забезпечення.

3. Для забезпечення успішної реалізації вказаних вище заходів, обов'язковою умовою є вирішення питання щодо забезпечення відповідних держаних програм саме національними висококваліфікованими кадрами, можливий вербувальний контакт яких з іноземними спецслужбами та організаціями був би мінімізований ще на стадії навчання. Це, своєю чергою, можливе лише через створення на державному рівні умов, що мотивували б вітчизняних висококваліфікованих фахівців у сфері високих технологій до роботи в Україні безпосередньо після закінчення ними вищих навчальних закладів і співробітництва найбільш талановитих студентів з профільними науково-дослідними установами ще під час навчання.

Список використаних джерел

1. EU Serious and Organised Crime Threat Assessment (SOCTA 2013) / [Electronic resourse]. – Mode of access :

https://www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta.

2. Правоохоронці знешкодили міжнародну злочинну групу хакерів / [Електронний ресурс]. – Режим доступу :

http://mvs.gov.ua/mvs/control/main/uk/publish/article/1069179.

3. В Сети обнаружен компьютерный червь чрезвычайной сложности / [Электронный ресурс]. – Режим доступа :

http://www.kaspersky.ru/news?id=207733976.

4. Создатели вредоносов бьют рекорды – 160 тыс. новых образцов ежедневно / [Электронный ресурс]. – Режим доступа :

http://ko.com.ua/sozdateli_vredonosov_byut_rekordy_160_tys_novyh_obrazcov_ezhednevno_105433.

5. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" : Указ Президента України від 1 трав. 2014 р. № 449/2014 / [Електронний ресурс]. – Режим доступу :

http://zakon2.rada.gov.ua/laws/show/449/2014.

6. Гавловський В. Д. До питання протидії використанню "шпигунських" програм-вірусів // Актуальні проблеми управління інформаційною безпекою держави : зб. матер наук.-практ. конф. : [у 2 ч.] (м. Київ, 20 берез. 2014 р.). – К. : Центр навч.-наук. та наук.-практ. вид. НА. СБ України, 2014. – Ч. 2. – С. 87–91.

7. Кримінальний кодекс України (КК України). Науково-практичний коментар / [Електронний ресурс]. – Режим доступу : http://uazakon.ru/ukr/bku/361(1)/default.htm.

8. "Лаборатория Касперского" взломала шпионскую сеть "Красный Октябрь" миру / [Электронный ресурс]. – Режим доступа : http://russian.rt.com/article/3020.

9. MiniDuke – новая вредоносная программа для кибершпионажа в государственных структурах по всему миру / [Электронный ресурс]. – Режим доступа : http://www.kaspersky.ru/news?id=207733960.

10. Во втором квартале число мобильных зловредов еще больше возросло [Электронный ресурс] // InternetUA. – 2013. – 17 авг. – Режим доступа : http://internetua.com/vo-vtorom-kvartale-csislo-mobilnih-zlovredov-esxe-bolshe-vozroslo.

11. Маски сорваны: "Лаборатория Касперского" раскрывает сложнейшую глобальную кампанию кибершпионажа / [Электронный ресурс]. – Режим доступа : http://www.kaspersky.ru/about/news/virus/2014/maski-sorvani-kaspersky-lab-starts-global-company-cyber-espionage.

12. Icefog: новая кибершпионская кампания "по найму" / [Электронный ресурс]. – Режим доступа : http://business.kaspersky.ru/icefog-novaya-kibershpionskaya-kampaniya-po-najmu/.

13. Немецкие IT-специалисты обнаружили разработанный россиянами руткит // InternetUA / [Электронный ресурс]. – Режим доступа : http://internetua.com/nemeckie-IT-specialisti-obnarujili-razrabotannii-rossiyanami-rutkit).

14. В Литве призывают готовится "к кибервойне с Востоком" / [Электронный ресурс]. – Режим доступа : http://www.regnum.ru/news/fd-abroad/ukraina/1791312.html.

15. "Лабораторія Касперського" аналізує зв'язок між собою кібершпигунів / [Електронний ресурс]. – Режим доступу : http://rovno.ua/archives/1065.

16. Специалисты говорят о новом суперсложном вредоносе Turla / [Электронный ресурс]. – Режим доступа : http://www.cybersecurity.ru/crypto/189807.html.

17. Лучший киберсыщик России срывает планы американских шпионов и помогает кремлевским приятелям / [Электронный ресурс]. – Режим доступа : http://www.inopressa.ru/article/24jul2012/wired/kaspersky.html.

18. Український національний антивірус – захист від 100 тисяч "бацил" / [Електронний ресурс]. – Режим доступу : http://old.dailylviv.com/news/2575.

19. Рейтинг антивирусов 2014. Пресс-релизы TrustPort / [Электронный ресурс]. – Режим доступа : http://trustport.com.ua/press-release.html.

20. У столиці працює 18 тис. IT-фахівців / [Електронний ресурс]. – Режим доступу : http://www.eveningkiev.com/ua/19081/news/1394806650.html.

21. Досягнення студентів факультету кібернетики у фіналах чемпіонату світу з програмування, командна першість / [Електронний ресурс]. – Режим доступу : http://cyb.univ.kiev.ua/world-cup-final.html.

На основе проведенного анализа, в контексте проблем защиты национальной безопасности Украины в информационной сфере, приводится аргументация о необходимости разработки и реализации комплекса организационно-практических мер противодействия противоправному использованию вредоносного программного обеспечения, а также разработки национального антивирусного программного обеспечения.

Based on the analysis, in the context of the national security of Ukraine protection in the information sphere, the argument on the need for the development and implementation of a range of organizational and practical measures to counteract illegal using of malicious software and the development of the national antiviral software are given.

Стаття надійшла до редакції журналу 28 травня 2014 року.