УДК 004.056

В.В. Умінський, к.т.н., п.н.с.
Житомирський військовий інститут ім. С.П. Корольова
Національного авіаційного університету

КЛАСИФІКАЦІЯ ЗАСОБІВ СПЕЦІАЛЬНОГО ПРОГРАМНОГО ВПЛИВУ НА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ

В роботі запропонована нова класифікація засобів спеціального програмного впливу із врахуванням сучасних тенденцій їх розвитку, наведено основні принципи функціонування цих засобів.

Постановка проблеми у загальному вигляді та її зв'язок із важливими практичними завданнями. Одним з напрямів комп'ютерного радіоелектронного подавлення виступає програмне подавлення інформаційно-телекомунікаційних систем (ІТС). Під програмним подавленням ІТС розуміється комплекс організаційно-технічних заходів, спрямованих на порушення нормального функціонування ІТС шляхом застосування до них засобів спеціального програмного впливу (СПВ) [1].

Засоби СПВ на логічному рівні являють собою хибні програми, процедури, дані. З фізичної точки зору засоби СПВ – це спеціальні заважаючі дії на ІТС, подібні по розпізнавальних параметрах дійсним сигналам [1].

Для організації протидії засобам СПВ необхідне знання принципів функціонування останніх, що можливе за рахунок чіткої та однозначної їх класифікації.

Аналіз останніх досліджень і публікацій. Як правило, кожна компанія, що займається розробкою антивірусних засобів, має свою класифікацію [2–6]. Наслідком цього є декілька назв одного й того ж засобу СПВ, що ускладнює розуміння алгоритму його роботи. Крім того, сучасні засоби СПВ вже не є простими і можуть поєднувати ознаки відомих в літературі «вірусів», «троянських конів» та «мережевих хробаків» [2].

Метою статті є узагальнення існуючих класифікацій засобів СПВ, виділення в них загальних ознак та побудова уніфікованої класифікації, яка задовольнить вимогам усіх провідних компаній по розробці антивірусних програм.

Викладення основного матеріалу. Всі засоби СПВ можна поділити за такими ознаками:

- за об'єктом впливу;
- за видом деструктивної дії;
- за середовищем розповсюдження;
- за середовищем існування;
- за можливістю саморозмноження
- за можливістю укриття факту присутності;
- за часом знаходження в оперативній пам'яті ЕОМ;
- за операційною системою.

Розглянемо класифікацію засобів СПВ за вказаними ознаками та особливості функціонування кожного із цих засобів.

Залежно від об'єкта, на який спрямований засіб СПВ, останній підрозділяється на: засіб впливу на програмне забезпечення, дані, апаратну частину і оператора ІТС.

Засіб СПВ на програмне забезпечення. В результаті дії засобів СПВ на ІТС змінюються характеристики і алгоритми роботи наявного в пам'яті системи програмного забезпечення. Деякі програми можуть бути стерті або модифіковані. Модифікація програм можлива як із збереженням властивих ним функцій, так і зі зміною їх. Викликані зміни породжують різні помилки, збої або відмови в роботі програмного забезпечення.

Засіб СПВ на дані призводить до видалення, модифікації або підміни дійсних даних помилковими, що приводить до отримання спотвореного результату.

Засіб СПВ на апаратну частину ІТС дозволяє змінити характеристики апаратних засобів, їх стан, або вивести апаратні засоби з ладу. Прикладом таких дій є: інтенсивне використання погано охолоджуваного елемента конструкції для виведення його з ладу в результаті перегріву, "пропалювання" плями на екрані, порушення роботи периферійного устаткування, шляхом завдання йому неправильних режимів функціонування тощо.

Засіб СПВ на операторів спрямований на дезінформацію персоналу ІТС або на зміну його психофізіологічного стану за рахунок прихованої дії спеціальних оптичних і звукових сигналів. В результаті дії даного типу засобів можуть ухвалюватися невірні рішення, а іноді оператор взагалі не в змозі буде виконувати свої функціональні обов'язки.

За видом **деструктивної дії** розрізняють такі засоби СПВ.

Утиліта віддаленого адміністрування комп'ютерів в мережі (Backdoor*)*. За своєю функціональністю вона багато в чому нагадує різні системи адміністрування, що розробляються і поширюються фірмами-виробниками програмних продуктів.

Особливістю цієї програми є відсутність попередження про інсталяцію і запуск. При запуску *Backdoor* встановлює себе в системі і потім стежить за нею, про що користувач не здогадується. Посилання на програму може бути відсутнім в списку активних додатків, внаслідок чого користувач не знає про її присутність в системі, тоді як його комп'ютер відкритий для видаленого управління.

Утиліта прихованого управління дозволяє робити з комп'ютером все, що в неї заклав автор: приймати або відправляти файли, запускати і знищувати їх, виводити повідомлення, стирати інформацію, перезавантажувати комп'ютер тощо. В результаті *Backdoor* може бути використаний для виявлення і передачі конфіденційної інформації, запуску інших засобів СПВ, знищення даних і т.п.

Крадіжка паролів (PSW). Дане сімейство об'єднує програми, що «крадуть» різну інформацію із зараженого комп'ютера, зазвичай – системні паролі (PSW — Password-Stealing-Ware). При запуску *PSW*-програми шукають системні файли, що зберігають різну конфіденційну інформацію, і посилають її по вказаній в коді *PSW*-програми електронній адресі або адресам.

Існують *PSW*-програми, які повідомляють і іншу інформацію про заражений комп'ютер, наприклад, інформацію про систему (розмір пам'яті і дискового простору, версія операційної системи), тип використовуваного поштового клієнта, IP-адресу і т.п. Деякі програми даного типу «крадуть» реєстраційну інформацію до різного програмного забезпечення.

Інтернет-клікери (Clicker). Сімейство програм, основна функція яких – організація несанкціонованих звернень до інтернет-ресурсів (зазвичай до Web-сторінок). Досягається це або видачею відповідних команд браузеру, або заміною системних файлів, в яких вказані «стандартні» адреси інтернет-ресурсів (наприклад, файл hosts в MS Windows).

Цілями для подібних дій можуть бути наступні:

- організація DoS-атаки (Denial of Service) на будь-який сервер;
- впровадження на інші комп'ютери засобів СПВ.

Завантажувачі (Downloader) – доставка інших засобів СПВ. Програми цього класу призначені для завантаження і установки на комп'ютер, що атакується, нових версій засобів СПВ. Завантажені програми або запускаються на виконання, або реєструються на автозавантаження відповідно до можливостей операційної системи. Вказані дії відбуваються без відома користувача.

Інформація про імена і розташування завантажуваних програм міститься в коді *Downloader* або викачується з управляючого інтернет-ресурсу.

Інсталятори (Dropper) – інсталятор інших засобів СПВ. Програми цього класу написані з метою скритної інсталяції програм і практично завжди використовуються для установки на зараженому комп'ютері інших засобів СПВ. Фактично інсталятори є своєрідними архівами, всередині яких розміщується будь-який засіб СПВ.

Інсталятор зазвичай без будь-яких повідомлень (або з хибними повідомленнями про помилку в архіві або невірній версії операційної системи) завантажує на диск в будь-який каталог (у корінь диска C, в тимчасовий каталог, в каталоги Windows) інші файли і запускає їх на виконання.

Структура таких програм:

Основний код
Файл 1
Файл 2
...

«Основний код» виділяє зі свого файла решту компонентів (файл 1, файл 2, ...), записує їх на диск і запускає на виконання.

Хоча б один з компонентів є засобом СПВ, і як мінімум один компонент є «обманкою»: програмою-жартом, грою, картинкою або чимось подібним. «Обманка» відволікає увагу користувача або демонструє те, що файл, який запускається, дійсно робить щось «корисне», тоді як засіб СПВ інсталюється в систему.

В результаті використання програм даного класу досягається дві мети:

- прихована інсталяція засобів СПВ;
- захист від антивірусних програм, оскільки не всі з них в змозі перевірити всі компоненти усередині файлів цього типу.

Проксі-сервер (Proxy). Сімейство програм, що скритно здійснюють анонімний доступ до різних інтернет-ресурсів. Зазвичай використовуються для розсилки спаму.

Шпигунські програми (Spy). Даний засіб СПВ здійснює електронне шпигунство за користувачем зараженого комп'ютера: інформація, що вводиться з клавіатури, знімки екрана, список активних додатків і дії користувача з ними зберігаються у файлі на диску і періодично відправляються зловмисникові.

Укриття присутності в операційній системі (Rootkit). Поняття *rootkit* прийшло з UNIX. Первинно це поняття використовувалося для позначення набору інструментів, вживаних для отримання прав. На сьогоднішній день інструменти типу *rootkit* є і в інших операційних системах.

Rootkit – програмний код або техніка, спрямована на укриття присутності в системі певних об'єктів (процесів, файлів, ключів реєстру тощо).

«Бомби» в архівах (ArcBomb) є архівами, оформленими так, щоб викликати нештатну поведінку архіваторів при спробі розархівувати дані – зависання або істотне уповільнення роботи комп'ютера, заповнення диска великою кількістю «порожніх» даних. Особливо небезпечні *ArcBomb* для файлових і поштових серверів. Якщо на сервері використовується будь-яка система автоматичної обробки вхідної інформації, *ArcBomb* може просто зупинити роботу сервера.

Оповіщувач (Notifier) – оповіщення про успішну атаку. Програми даного типу призначені для повідомлення атакуючої особи про заражений комп'ютер. У повідомлення, що відправляється, заноситься інформація про комп'ютер, наприклад, IP-адреса комп'ютера, номер відкритого порту, адреса електронної пошти і т.п. Відправка здійснюється різними способами: електронним листом, спеціально оформленим зверненням до Web-сторінки порушника, ICQ-повідомленням.

Дані програми використовуються в багатокомпонентних засобах СПВ для оповіщення порушника про успішну інсталяцію компонент в систему, що атакується.

Мережевий аналізатор трафіка (Sniffer). Програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіка, призначеного для інших вузлів.

Під час роботи *аналізатора* мережевий інтерфейс перемикається в так званий «режим прослуховування», що і дозволяє йому отримувати пакети, адресовані іншим інтерфейсам в мережі.

Перехоплення трафіка може здійснюватися:

– звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів замість комутаторів, інакше метод малоефективний, оскільки на *аналізатор* потрапляють лише окремі фрейми);

– підключенням *аналізатора* в розрив каналу;

– відгалуженням (програмним або апаратним) трафіка і спрямуванням його копії на *аналізатор*;

– через аналіз побічних електромагнітних випромінювань і відновлення трафіка, що прослуховується;

– через атаку на канальному або мережевому рівні, що призводить до перенаправлення трафіка жертви або всього трафіка сегменту на *аналізатор* з подальшим поверненням трафіка в належну адресу.

Мережеві атаки (DoS). Програми даного типу реалізують атаки на видаленні сервера, посилаючи на них численні запити, що призводить до відмови в обслуговуванні, якщо ресурси сервера, що атакується, недостатні для обробки всіх запитів, що поступають.

Знищення (відмова) устаткування можливе шляхом зміни його характеристик функціонування або порушення роботи драйверів.

Шифрування даних – найбільш складний метод деструктивних дій, який полягає в тому, що вміст файлів певних типів шифрується із застосуванням несиметричних алгоритмів шифрування з достатньо великими ключами.

Знищення (модифікація) даних. За одну з найбільш поширених деструктивних дій вважається знищення інформації (програм і даних). З погляду принципів роботи можна виділити декілька алгоритмів реалізації даної дії:

– видалення файлів за заданими умовами, наприклад, з певної папки, з певним розширенням, з певним ім'ям тощо;

– рекурсивне видалення або пошкодження всіх файлів на диску, наприклад, урізання розміру файла до нульової довжини, заміна вмісту файла, необоротне стирання файлів;

– низькорівневе пошкодження даних на жорсткому диску, наприклад, форматування диска, знищення boot- або MBR-сектора диска;

– пошкодження реєстру.

Окрім знищення, засоби СПВ можуть здійснювати зміну (модифікацію) вмісту файлів. Зміни в програмах породжують помилки, збої і відмови в роботі програмного забезпечення. Зміни у файлах Microsoft Office призводять до втрати важливої інформації.

Створення перешкод в роботі оператора – вид засобів СПВ, які не наносять безпосереднього збитку інформації і даним, що зберігаються на ЕОМ, але ускладнюють роботу оператора. Це може привести до прийняття невірного рішення, порушення термінів виконання поставленого завдання, а у ряді випадків – до невиконання його взагалі. До створюваних засобами СПВ перешкод можна віднести наступні:

– видача неправдивих, дратівливих або відволікаючих повідомлень;

– створення сторонніх звуків і візуальних ефектів;

- інсценування помилок або збоїв в програмі або в операційній системі;
- перезавантаження або зависання програм чи систем;
- блокування доступу до системних ресурсів;
- зменшення об'єму оперативної пам'яті і завантаження процесора зайвими завданнями, що уповільнюють роботу ЕОМ.

За **середовищем розповсюдження** розрізняють локальні і мережеві засоби СПВ. *Локальні* засоби СПВ здійснюють свої деструктивні дії в межах ЕОМ, що подавляється, незалежно від того, підключена вона до будь-якого виду комп'ютерної мережі чи ні. Вони не можуть самостійно уразити комп'ютерну мережу і не несуть ніякої небезпеки для інших засобів ІТС унаслідок відсутності механізму мережевого розповсюдження. Для зараження інших засобів ІТС користувач власноручно повинен перенести заражені об'єкти з одного комп'ютера на інший.

Велику небезпеку представляють *мережеві* засоби СПВ. У літературі ці засоби відомі як «мережеві черв‘яки». Для свого розповсюдження в ІТС вони активно використовують протоколи і можливості локальних і глобальних мереж. Мережеві засоби СПВ проникають на комп'ютери ІТС без будь-яких дій з боку користувача. Основним принципом роботи мережевого засобу є можливість самостійно передати свій код на видалений сервер або робочу станцію і, по можливості, запустити свій код на виконання або підштовхнути користувача до запуску зараженого файла.

Залежно від виду використовуваної мережі для розповсюдження засоби СПВ поділяються на:

E-mail (поштові). До даної категорії програм відносяться ті з них, які для свого розповсюдження використовують електронну пошту. При цьому засіб СПВ посилає або свою копію у вигляді вкладення в електронний лист, або посилання на свій файл, розташований на будь-якому мережевому ресурсі.

У першому випадку код програми активізується при відкритті зараженого вкладення, в другому – при відкритті посилання на заражений файл. У обох випадках ефект однаковий – активізується код засобу СПВ.

Для відправки заражених повідомлень поштові засоби СПВ використовують різні способи. Найбільш поширені:

- пряме підключення до SMTP-сервера, використовуючи вбудовану в код програми поштову бібліотеку;
- використання сервісів MS Outlook;
- використання функцій Windows MAPI.

Для пошуку поштових адрес, на які розсилатимуться заражені листи, використовуються такі методи:

- розсилка по всіх адресах, виявлених в адресній книзі MS Outlook;
- зчитування адрес з адресної бази WAB;
- сканування файлів на диску і виділення в них рядків, що є адресами електронної пошти;
- розсилка по адресах, виявлених в листах у поштовій скриньці.

ІМ-засоби СПВ, що використовують інтернет-пейджери. Програми даного типу використовують єдиний спосіб розповсюдження – розсилку на виявлені в контакт-аркуші контакти повідомлень, що містять URL-посилання на файл, розташований на будь-якому Web-сервері. Даний прийом практично повністю повторює аналогічний спосіб розсилки, що використовується поштовими засобами СПВ.

P2P-засоби СПВ для файлообмінних мереж. Механізм роботи більшості подібних програм полягає у впровадженні їх в P2P-мережу шляхом копіювання в каталог обміну файлами, розташований на локальній машині. Подальшим розповсюдженням засобу СПВ займається P2P-мережа шляхом надання користувачам необхідного сервісу для скачування файла із зараженого комп'ютера.

IRC-засоби СПВ в IRC-каналах. У даного типу засобів існує два способи розповсюдження, подібні тим, що використовують поштові засобів СПВ. Перший полягає у відсиланні URL-посилання на копію засобу СПВ. Другий спосіб – відсилання зараженого файла будь-якому користувачеві мережі. При цьому користувач, що атакується, повинен підтвердити прийом файла, зберегти його на диск і запустити на виконання.

NET. Існує ряд інших способів зараження видалених комп'ютерів, які в даній класифікації отримали назву NET. Наприклад:

- копіювання засобу СПВ на мережеві ресурси;
- проникнення засобу СПВ на комп'ютер через уразливості в операційних системах і додатках;
- проникнення в мережеві ресурси публічного використання;
- паразитування на інших засобах СПВ.

Перший спосіб полягає в тому, що засіб СПВ шукає видалені комп'ютери і копіює себе в каталоги, відкриті на читання і запис (якщо такі виявлені). При цьому засоби даного типу або перебирають доступні мережеві каталоги, використовуючи функції операційної системи і/або випадковим чином шукають комп'ютери в глобальній мережі, підключаються до них і намагаються відкрити їх диски на повний доступ.

Для проникнення другим способом засоби СПВ шукають в мережі комп'ютери, на яких використовується програмне забезпечення, що містить критичні уразливості. Для зараження уразливих комп'ютерів засіб СПВ посилає спеціально оформлений мережевий пакет або запит (експлойт уразливості), внаслідок чого код (або частина коду) даного засобу проникає на комп'ютер-жертву. Якщо мережевий пакет містить тільки частину коду засобу СПВ, він потім викачує основний файл і запускає його на виконання.

Окрему категорію складають засоби СПВ, що використовують для свого розповсюдження Web- і FTP-сервера. Зараження відбувається у два етапи: проникнення в комп'ютер-сервер і модифікація службових файлів сервера (наприклад, статичні Web-сторінки); очікування відвідувачів зараженого сервера і проникнення.

Існують засоби СПВ, що паразитують на інших мережевих засобах і/або розглянутих вище програмах видаленого адміністрування (Backdoor). Дані програми використовують той факт, що багато Backdoor дозволяють по певній команді викачувати вказаний файл і запускати його на локальному диску. Те ж саме можливо з деякими мережевими засобами СПВ, що містять Backdoor-процедури. Для зараження видалених комп'ютерів дані засоби СПВ шукають інші комп'ютери в мережі і посилають на них команду скачування і запуску своєї копії.

Залежно від **середовища існування** всі засоби СПВ поділяються на дві групи: файлові і завантажувальні.

Файлові засоби СПВ при своєму розмноженні використовують файлову систему операційної системи. На відміну від файлових *завантажувальні* засоби СПВ ґрунтуються на алгоритмах запуску операційних систем або алгоритмах ініціалізації дискет, CD/DVD, а також флеш дисків.

У свою чергу, файлові засоби СПВ класифікуються по типах файлів (бібліотеки, драйвери, системні, виконувані, макро, скриптові файли), в яких вони зберігаються, переносяться і розмножуються, а також за місцем розташування відносно цих файлів (перезаписуючі, паразитичні, супроводжуючі, автономні).

Перезаписуючі засоби СПВ. Даний метод зараження є найбільш простим: засіб СПВ записує свій код замість коду файла, що заражається, знищуючи його вміст. При цьому файл перестає працювати і не відновлюється. Такі засоби дуже швидко виявляють себе, оскільки операційна система і додатки досить швидко перестають працювати.

До *паразитичних* відносяться всі файлові засоби СПВ, які при розповсюдженні обов'язково змінюють вміст файлів, залишаючи самі файли при цьому повністю або частково працездатними. Основними типами таких засобів СПВ є засоби, що записуються в початок файлів, в кінець файлів і в середину файлів.

До *супроводжуючих* засобів СПВ відносяться дві категорії: програми-компаньйони і програми-посилання. *Програми-компаньйони* – засоби СПВ, які не змінюють файли, що заражаються. Їх алгоритм роботи полягає в тому, що для файла, що заражається, створюється файл-двійник. При запуску зараженого файла управління отримує файл-двійник.

Програми-посилання також не змінюють фізичного вмісту файлів, проте при запуску зараженого файла «примушують» операційну систему виконати свій код шляхом модифікації необхідних полів файлової системи.

Автономні файлові засоби СПВ не здійснюють зараження файлів в системі. Вони існують на правах окремого файла, не прив‘язуючись до будь-яких об‘єктів операційної системи. Іноді ці засоби СПВ дають своїм копіям спеціальні назви, щоб підштовхнути користувача до свого запуску (наприклад, Instal.exe).

Завантажувальні засоби СПВ можуть вражати завантажувальні сектори жорсткого диска (вінчестера), дискети, CD/DVD диска або флеш диска, а також головний завантажувальний запис (MBR – Master Boot Record) жорсткого диска.

Зараження дискет, CD/DVD дисків або флеш дисків здійснюється єдиним відомим способом – засіб СПВ записує свій код замість оригінального коду boot-сектора носія.

Вінчестер заражається трьома можливими способами – засіб СПВ записується або замість коду MBR, або замість коду boot-сектора завантажувального диска (зазвичай диска C:), або модифікує адресу активного boot-сектора в таблиці розділів диска (Disk Partition Table), розташованій в MBR вінчестера.

Однією з основних ознак засобів СПВ, що визначають їх ступінь небезпеки, є **здібність до саморозмноження**. За даною ознакою всі засоби СПВ підрозділяються на ті, що саморозмножуються (відомі в літературі як комп'ютерні віруси і мережеві черв'яки) і ті, що самі не розмножуються.

До *саморозмножувальних* відносяться ті, які можуть копіювати себе, створюючи нові програмні об'єкти, що володіють властивістю саморозмноження. Створювані нові програмні об'єкти можуть абсолютно повторювати вихідні (мережеві черв'яки), а можуть модифікуватися, істотно відрізняючись від первинного засобу СПВ (віруси).

З метою приховування слідів своєї присутності в комп'ютері і нанесення більшого збитку засоби СПВ можуть використовувати ряд алгоритмів, що роблять їх невидимими для користувача і

спеціалізованого програмного забезпечення (антивірусних програм). Залежно від наявності механізму **приховування факту присутності** засоби СПВ класифікуються як *масковані* (стелс) і *немасковані*. Для маскування засоби СПВ можуть використовувати один з таких алгоритмів:

шифрування власного коду, що ускладнює їх дезассемлювання і виявлення в файлі або пам‘яті;

зміна власного програмного коду із збереженням деструктивних властивостей, що призводить до зміни сигнатури і неможливістю виявлення антивірусною програмою;

перехоплення запитів операційної системи (переривань) до уражених файлів або секторів дисків і «підстановка» замість себе незаражених ділянок інформації. Таким чином, до певного моменту засоби СПВ можуть залишатися непоміченими, виконуючи деструктивні дії і вражаючи все більшу кількість файлів;

розбиття на пакети – найбільш розповсюджений на сьогоднішній день алгоритм прихованого проникнення засобів СПВ на ПЕОМ через мережеві засоби. Сутність цього алгоритму полягає в тому, що засіб СПВ розбивається на дрібні пакети, структура яких жодним чином не містить ознак засобу СПВ, і тому не можуть бути виявлені антивірусними програмами. Після проникнення па ПЕОМ-«жертву» пакети збираються в єдину програму, яка виконує свої деструктивні функції;

знищення антивірусних засобів, що призводить до неуможливлювання виконання функції пошуку та локалізації засобів СПВ, хоча за зовнішніми ознаками користувач не здатен цього виявити.

Для виконання будь-яких дій в ураженій ІТС засіб СПВ повинен отримати управління, тобто необхідно запустити процес, пов'язаний з цим засобом. Всі виконувані процеси, у тому числі і пов'язані із засобами СПВ, знаходяться в оперативній пам'яті комп'ютера. Залежно від часу **знаходження в оперативній пам'яті** засоби СПВ поділяються на резидентні і нерезидентні.

Резидентні – знаходяться в оперативній пам'яті постійно з деякого моменту часу до закінчення сеансу роботи ЕОМ (виключення живлення або перевантаження).

Нерезидентні – починають роботу по аналогічній події, але закінчують її самостійно по закінченню деякого проміжку часу або деякій події, при цьому вивантажуючи себе з оперативної пам'яті цілком.

Кожен засіб СПВ заражає файли тільки певної операційної системи і не здатні завдати збитку ІТС, що функціонує під управлінням інших операційних систем. Саме ця обставина покладена в основу класифікації засобів СПВ **по операційній системі**.

Висновки. Запропонована класифікація відповідає основним принципам розподілу об‘єктів за ознаками, узагальнює досвід провідних антивірусних лабораторій та може розвиватись шляхом введення нових ознак або розрядів в існуючі ознаки. Віднесення засобу СПВ до певного класу за кожною ознакою даної класифікації дозволяє усвідомити алгоритм його функціонування, а значить, побудувати ефективну систему захисту.

ЛІТЕРАТУРА:

1. Методы и средства защиты информации: В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко / Под ред. В.А. Хорошко. – К.: Арий, 2008.
2. Шестой саммит вирусных аналитиков «Лаборатории Касперского»: репортаж с открытого пресс-дня. http://www.ixbt.com/cm/kaspersky-summit2k7.shtml.
3. Классические вирусы. http://anticod.ucoz.ru.
4. http://www.viruslist.com.
5. Классификация вредоносов. http://av-school.ru.
6. Современные типы компьютерных вирусов и других вредоносных программ. http://www.getinfo.ru.

УМІНСЬКИЙ Володимир Вікторович – кандидат технічних наук, провідний науковий співробітник наукового центру Житомирського військового інституту ім. С.П. Корольова Національного авіаційного університету.

Наукові інтереси:

– автоматизовані системи;

– системи захисту інформації.

Подано 07.04.2009

Умінський В.В. Класифікація засобів спеціального програмного впливу на інформаційно-телекомунікаційні системи
Уминский В.В. Классификация средств специального программного воздействия на информационно-телекомуникационные системы.
Uminskiy V.V. Classification of tools of the special programmatic affecting information-telecommunications systems.

УДК 004.056

Классификация средств специального программного воздействия на информационно-телекомуникационные системы / В.В. Уминский

В работе предложена новая классификация средств специального программного воздействия с учетом современных тенденций их развития, приведены основные принципы функционирования этих средств.

УДК 004.056

Classification of tools of the special programmatic affecting information-telecommunications systems / V.V. Uminskiy

New classification of tools of the special programmatic influence is in-process offered taking into account modern their progress trends, basic principles of functioning of these tools are resulted.