УДК 355.02

І.В. Пампуха,
кандидат технічних наук, доцент,
С.П. Гришин,
кандидат технічних наук,
О.В. Мірошніченко,
кандидат технічних наук

СУЧАСНІ ПРОБЛЕМИ ТЕХНОЛОГІЧНОЇ БЕЗПЕКИ ПРОГРАМНИХ ЗАСОБІВ СИСТЕМ УПРАВЛІННЯ ОЗБРОЄННЯМ ТА ВІЙСЬКОВОЮ ТЕХНІКОЮ

Безпека програмного забезпечення складних систем військового призначення пов'язана з потенційною можливістю внесення до програмних засобів навмисних дефектів або спеціальних програмних засобів, які служать для цілеспрямованої прихованої дії на технічну або інформаційну систему, у складі якої використовується ЕОМ. Тому інформація щодо можливих наслідків їх втілення та методів захисту від них є дуже актуальною.

***Ключові слова**: технологічна безпека, інформаційна система, шкідливе програмне забезпечення, стійкість систем сучасної зброї.*

Безопасность программного обеспечения сложных систем военного назначения связана с потенциальной возможностью внесения в программные средства преднамеренных дефектов или специальных программных средств, которые служат для целенаправленного скрытого воздействия на техническую или информационную систему, в составе которой используется ЭВМ. Поэтому информация относительно возможных последствий их внедрения и методов защиты от них остается очень актуальной.

***Ключевые слова**: технологическая безопасность, информационная система, вредное программное обеспечение, стойкость систем современного оружия.*

Software security of the complex systems for military purposes is related to the potential possibility for bringing in the software purposeful defects or special software tools that are used to focus the hidden impact on the technical or informational system, which uses computers. Therefore, an information on the possible effects of their introduction and methods of the protection from them is very important.

***Keywords:** technological security, information system, harmful software, resistance of the systems of modern weapons.*

За оцінками експертів, на сьогодні склалася ситуація, коли бойові можливості і стійкість систем сучасної зброї визначаються показниками якості і надійності програмних засобів (більшою мірою порівняно з апаратними засобами). Програмне забезпечення стає джерелом уразливості сучасних оборонних систем, а використання програмних засобів у складі систем зброї, бойового управління і зв'язку,

а також інших критичних систем породжує нову проблему – забезпечення технологічної безпеки програмних засобів військового призначення. Навіть приблизний аналіз показує стійке значне збільшення відносної долі завдань і функцій, що виконуються за допомогою програмних засобів порівняно з апаратними. Таким чином, зараз склалася ситуація, коли бойові можливості і стійкість систем сучасної зброї великою мірою визначаються показниками якості і надійності програмних засобів. У зв'язку з цим, деякі західні авторитетні вчені висловлювали думки про те, що відмови програмного забезпечення, яке входить до складу системи бойового управління стратегічними силами і засобами, потенційно можуть стати детонаторами ядерного конфлікту.

Метою статті є висвітлення основних проблем забезпечення технологічної безпеки програмних засобів військового призначення та можливих шляхів їх вирішення.

Аналіз останніх досліджень і публікацій показує безперервне підвищення вимог до якості програмних компонентів сучасних і перспективних засобів збройної боротьби, пояснюючи це бурхливими взаємопов'язаними процесами комп'ютеризації й інтелектуалізації відповідних систем ураження. Неминучим наслідком цього стає різке збільшення обсягів застосування і трудомісткості програмних засобів, які використовуються в ЕОМ, системах зброї, автоматизованих системах бойового управління і зв'язку, допоміжних і забезпечувальних системах військового призначення.

Вперше така проблема виникла в середині 60-х років. У той час фахівці, що створювали системи обробки інформації і управління, зіткнулися з новим явищем. Виявилось, що надійність їх функціонування залежить від програм, які виконуються в цей момент на ЕОМ. Доопрацювання або заміна програм дозволяла ліквідувати деякі відмови, хоча могла призвести до виникнення відмов іншого виду. Зараз безпека програмного забезпечення складних систем (в першу чергу військового призначення) пов'язана з потенційною можливістю внесення до програмних засобів навмисних дефектів або спеціальних програмних засобів (комп'ютерних вірусів, логічних бомб, "троянів", програмних закладок і т. і.), які служать для цілеспрямованої прихованої дії на технічну або інформаційну систему, у складі якої використовується ЕОМ. Особливо багато незручностей в останній час завдають комп'ютерні віруси, кількість яких сьогодні сягає 3 мільйонів. Тому інформація щодо можливих наслідків їх втілення та методів захисту від них залишається дуже актуальною. На щастя, велику групу реальних вірусів складають нешкідливі, які не порушують роботу ПЕОМ. Їх авторами зазвичай є старшокласники, студенти та ті, хто прагне підвищити свою кваліфікацію в галузі програмування. Серед вірусів, що порушують режим функціонування комп'ютера, є безпечні (які не ушкоджують файлову структуру), небезпечні (які ушкоджують цю структуру) і дуже небезпечні (які виводять з ладу апаратуру). Ці віруси здебільшого конструюються професіоналами. Найбільшої шкоди з точки зору витоку інформації завдають криптовіруси, здатні пробити пролом навіть в такому потужному засобі оборони, як криптозахист. У момент введення електронного підпису криптовіруси перехоплюють секретні ключі і копіюють їх в задане місце. Більше того, при перевірці електронного підпису вони можуть викликати команду підтвердження достовірності свідомо неправильному підпису. І навіть при введенні в систему лише один раз, у момент генерації ключів, криптовірус призводить до

створення слабких ключів. Наприклад, при формуванні ключа на основі датчика випадкових чисел з використанням вбудованого таймера криптовірус може викликати зміну свідчень таймера з наступним поверненням в початковий стан. У результаті ключі легко розкрити. Сьогодні практично єдиний захист від таких криптовірусів – завантаження інформації з "чистого" носія і використання "чистого" (фірмового) програмного продукту. Але з іншого боку, навіть чистий програмний продукт може містити програмні закладки та інше ПЗ, призначене для виводу з ладу (збоїв у роботі) або для витоку важливої інформації.

Шкідливе ПЗ може бути досить ефективно застосовано у військових цілях як активний елемент інформаційно-кібернетичної протидії. При цьому, чим вище міра комп'ютеризації і інтелектуалізації систем військового призначення, тим більша вірогідність появи шкідливого ПЗ. Тому однією з сучасних особливостей проектування і розробки програмного забезпечення військового призначення є необхідність забезпечення його технологічної безпеки.

Проте при реалізації складного і багатоетапного процесу створення програмних засобів в їх склад навмисно може бути внесено спеціальне шкідливе ПЗ. При цьому розробник цього ПЗ (алгоритміст, програміст або системотехнік) може здійснювати такі дії або випадково, або навмисно. Останнє викликає особливу стурбованість відповідних спецслужб.

Шкідливе ПЗ може бути реалізоване у вигляді декількох команд і мати досить складний і "тонкий" механізм активізації, "налаштований" на умови реального бойового застосування системи зброї або на строго певну комбінацію вхідних даних. Ці програми можуть бути включені до складу як загального програмного забезпечення обчислювальної системи, так і спеціальних (прикладних) програмних засобів, що реалізовують алгоритм перетворення інформації.

У зарубіжній технічній літературі різновид шкідливого програмного забезпечення – програмні закладки підрозділяються на автоматичні і керовані. Перші, як правило, мають механізм спрацьовування, заздалегідь налаштований (прямо або побічно) на умови реального бойового застосування систем зброї або бойового управління, а останні мають механізм активізації, який контролюється ззовні (наприклад, за допомогою електронної закладки).

Виявити наявність програмної закладки у складі програмного забезпечення великого об'єму і складності дуже важко, оскільки вона може бути замаскована під реально існуючий алгоритм або його частину. Це посилюється повною невизначеністю про умови і момент спрацьовування програмної закладки, а також відсутністю прямих і непрямих ознак її наявності у складі програмного забезпечення.

Думка фахівців і виробників одностайна – програмні закладки, на відміну від поширених електронних, є витонченішими об'єктами ідеальної природи, що важко ідентифікуються. Обидва цих типа становлять особливу небезпеку для перспективних стратегічних оборонних систем. Наслідком активізації шкідливого ПЗ може бути повне або часткове порушення працездатності системи військового призначення, несанкціонований доступ до інформації автоматизованої системи (минувши комплекс засобів захисту і розмежування доступу), втрата або спотворення інформації в спеціальних банках даних і т. і. Найбільшу небезпеку вони становлять для систем зброї одноразового бойового застосування, наприклад ракетних комплексів стратегічного призначення, а також для систем бойового управління, що мають логічне розподілення каналів бойового і чергового режимів.

Експерти низки країн, аналізуючи вірогідні наслідки вживання шкідливого ПЗ, виявили, що одним з них може бути блокування можливості бойового застосування системи зброї певного класу або інформаційної системи військового призначення. Іншими словами, це означає, що, володіючи потужною зброєю для стримання потенційного противника, можна фактично опинитися беззбройним. Як ілюстрацію цієї ситуації можна привести військовий конфлікт в Перській затоці, коли при проведенні багатонаціональними силами операції "Буря в пустелі" система ППО Іраку виявилася заблокованою з невідомої причини. У результаті іракська сторона була змушена залишити без відповіді бомбові удари по своїй території. Не дивлячись на відсутність вичерпної інформації, багато іноземних фахівців висловлюють припущення, що ЕОМ, що входять до складу комплексу технічних засобів системи ППО, які купував Ірак у Франції, містили спеціальні керовані електронні закладки, що блокували роботу обчислювальної системи. Якщо вони мали рацію, то це означає, що саме з того часу розпочався етап практичного застосування нової електронно-інформаційної зброї.

Проблеми, пов'язані з розробкою програмних засобів, починають серйозно турбувати більшість країн світу. З метою збільшення обсягу виробництва і підвищення якості програмного забезпечення в США з середини 1983 року було розпочато декілька програм, в результаті реалізації яких було створено об'єднане автоматизоване середовище програмування, що охоплює весь життєвий цикл програмного забезпечення. Базою послужила цільова програма по створенню універсальної мови програмування високого рівня АДА. Завдяки її використанню стало можливим мати сумісні засоби розробки і супроводу програмного забезпечення, контролювати його надійність і безпеку. За твердженням Стефена Цейгера з Rational Software Corporation, розробка програмного забезпечення на АДА в цілому обходиться на 60 % дешевше, а розроблена програма має в 9 разів менше дефектів, чим при використанні Сі. Останні зміни у стандартах АДА були опубліковані в березні 2007 року. Вони торкнулись, в основному, можливостей об'єктно-орієнтованого програмування: введені інтерфейси, прийнятий звичайний для більшості гібридних мов синтаксис виклику метода, внесено низку доповнень.

Міністерство оборони США ще у 1994 році продемонструвало системне програмне забезпечення для високоживучих розподілених і паралельних обчислювальних систем. Технологія програмного забезпечення з високою гарантією надійності необхідна при проектуванні систем, критичних для безпеки особового складу і більшості систем зброї, а також захищених систем, в яких повинні гарантуватися конфіденційність і цілісність інформації.

Все це свідчить про те, що промислово розвинені країни украй обережно, на відміну від нас, відносяться до використання імпортних інформаційних технологій, підозрюючи наявність в них навмисних дефектів, що активізуються при певному поєднанні вхідних даних (азимут пуску ракети, курс літака, специфічна команда управління) з метою порушення роботи системи військового призначення. Дуже є цікавим і той факт, що американським законодавством жорстко обмежено вживання технічних і програмних засобів зарубіжного виробництва на користь забезпечення національної безпеки.

В цілому політику США в області технології програмування слід розцінювати як широкомасштабну стратегію протистояння в інформаційній сфері, переслідуючу

глобальні політичні і економічні цілі. Вона також передбачає створення одного з видів "несмертельної зброї" – спеціальних засобів дії на програмне забезпечення противника і засобів захисту від аналогічної дії з його боку.

Складність сучасного програмного забезпечення військового призначення полягає в тому, що в принципі не існує технологій створення програмної продукції без єдиного дефекту. Тому жодна організація-розробник не гарантує абсолютної надійності створюваного програмного продукту, знімаючи з себе всяку відповідальність за наслідки, до яких можуть привести дефекти в програмах.

Положення ускладнюється і тим, що можуть виникнути ситуації, коли не можна буде однозначно відповісти на питання: чи є виявлена програмна конструкція навмисною програмною закладкою або невмисним випадковим програмним дефектом навіть у тому випадку, коли встановлено, що активізація такої програмної конструкції викликає блокування можливості бойового застосування системи зброї за певних умов – із заданого моменту часу або по певній цілі (об'єктах). Це означає, що в автора шкідливого ПЗ є можливість уникнути повної юридичної відповідальності, використовуючи тонкощі розробки програмних засобів, що реалізують особливості алгоритмів і моделей.

Крім того, прогресуюча тенденція імпорту зарубіжних програмних засобів і інформаційних технологій призводить до збільшення вірогідності імпорту таких програмних дефектів.

Сучасні способи боротьби зі шкідливим ПЗ. На цей час для виявлення програмних закладок і випадкових програмних дефектів запропоновані антивірусні програми, що сигналізують про наявність підозрілого коду в завантажувальному секторі диска. З ініціацією статичної помилки на дисках добре справляється Disk Doctor, що входить в поширений комплект утиліт Norton Utilities. А засоби перевірки цілісності даних на диску типу ADinf, AVZ і т. і. дозволяють успішно виявляти зміни, що вносяться до файлів програмними закладками. Крім того, також ефективний пошук фрагментів кодів програмних закладок по характерних для них послідовностях нулів і одиниць (сигнатурах), а також дозвіл виконання лише програм з відомими сигнатурами.

Виявлення втіленого коду програмної закладки полягає у виявленні ознак його присутності в комп'ютерній системі. Ці ознаки можна розділити на наступні два класи: якісно-візуальні та ті, що виявляються засобами тестування і діагностики.

До якісно-візуальних ознак відносяться відчуття і спостереження користувача комп'ютерної системи, який помічає певні відхилення в її роботі (змінюються склад і довжини файлів, старі файли кудись пропадають, а замість них з'являються нові, програми починають працювати повільніше або закінчують роботу дуже швидко, або взагалі перестають запускатися). Не дивлячись на те, що думка про наявність ознак цього класу здається дуже суб'єктивною, проте, вони часто свідчать про наявність неполадок в комп'ютерній системі і, зокрема, про необхідність проведення додаткових перевірок присутності програмних закладок засобами тестування і діагностики.

Завдання захисту від програмних закладок може розглядатися в трьох принципово різних варіантах:

– не допустити втілення програмної закладки в комп'ютерну систему;

– виявити втілену програмну закладку;

– видалити втілену програмну закладку.

При розгляді цих варіантів захист від програмних закладок схожий із захистом комп'ютерних систем від вірусів. Як і в разі боротьби з вірусами, завдання вирішується за допомогою засобів контролю за цілісністю системних і прикладних програм, що запускаються, а також за цілісністю інформації, що зберігається в комп'ютерній системі, і за подіями, критичними для функціонування системи. Проте ці засоби дієві лише тоді, коли самі вони не схильні до впливу програмних закладок, які можуть:

нав'язувати кінцеві результати контрольних перевірок;

впливати на процес зчитування інформації і запуск програм, за якими здійснюється контроль;

змінювати алгоритми функціонування засобів контролю.

При цьому дуже важливо, щоб включення засобів контролю виконувалося до початку дії програмної закладки, або коли контроль здійснювався лише з використанням програм управління, що знаходяться в ПЗП комп'ютерної системи.

Цікавий метод боротьби з втіленням програмних закладок може бути використаний в інформаційній банківській системі, в якій циркулюють виключно файли-документи. Щоб не допустити проникнення програмної закладки через канали зв'язку, в цій системі не допускається прийом жодного виконуваного коду. Для розпізнавання подій типу "ОТРИМАНИЙ ВИКОНУВАНИЙ КОД" і "ОТРИМАНИЙ ФАЙЛ-ДОКУМЕНТ" застосовують контроль за наявністю у файлі заборонених символів: файл вважається таким, що містить виконуваний код, якщо у ньому присутні символи, які ніколи не зустрічаються у файлах-документах.

Конкретний спосіб видалення втіленої програмної закладки залежить від методу її втілення в комп'ютерну систему. Якщо це програмно-апаратна закладка, то слід перепрограмувати ПЗП комп'ютера. Якщо це завантажувальна, драйвер, прикладна, замаскована закладка або закладка-імітатор, то можна замінити їх на відповідний завантажувальний запис, драйвер, утиліту, прикладну або службову програму, отриману від джерела, заслуговуючого на довіру. Нарешті, якщо це виконуваний програмний модуль, то можна спробувати добути його початковий текст, прибрати з нього наявні закладки або підозрілі фрагменти, а потім наново відкомпилювати.

Універсальним засобом захисту від впровадження програмних закладок є створення ізольованого комп'ютера. Комп'ютер називається ізольованим, якщо виконані наступні умови:

в ньому встановлена своя система типу BIOS, що не містить програмних закладок;

операційна система перевірена на наявність в ній закладок;

достовірно встановлена незмінність BIOS і операційної системи для цього сеансу;

на комп'ютері не запускалися і не запускаються ніякі інші програми, окрім тих, які вже пройшли перевірку на присутність в них закладок;

виключений запуск перевірених програм в будь-яких інших умовах, окрім перелічених вище, тобто поза ізольованим комп'ютером.

Для визначення міри ізольованості комп'ютера може використовуватися модель ступінчастого контролю. Суть його полягає в такому. Спочатку

робиться перевірка, чи немає змін в BIOS. Потім, якщо все гаразд, прочитуються завантажувальний сектор диска і драйвери операційної системи, які, у свою чергу, також аналізуються на предмет внесення в них несанкціонованих змін. І нарешті, за допомогою операційної системи запускається драйвер контролю викликів програм, який стежить за тим, щоб в комп'ютері запускалися тільки перевірені програми.

Висновки

Не дивлячись на чималий перелік способів та засобів боротьби зі шкідливим програмним забезпеченням, що існує на цьому етапі, проблема забезпечення технологічної безпеки програмних засобів військового призначення примушує звертати на себе увагу практично щодня. Необхідно зауважити, що при розробці перспективних зразків "розумної зброї" (тобто при подальшій комп'ютеризації і інтелектуалізації систем військового призначення) виникає неминучий парадокс сучасного програмного забезпечення, який полягає в тому, що фундаментальне джерело технологічного прогресу одночасно є зростаючим джерелом технологічної уразливості.

Вірогідність цієї загрози в сучасній обстановці різко зростає внаслідок таких чинників:

уніфікації систем управління зброєю, що призводить, зокрема, до можливості ураження всього угрупування однотипної зброї одним навмисним диверсійним програмним дефектом або впливом;

масового імпорту обчислювальних засобів, мережевих структур, інформаційних технологій і програмних засобів;

недосконалості системи закупівлі ОВТ;

відсутності юридичних норм, що регламентують особливості розробки комп'ютеризованих і інтелектуалізованих високоточних систем зброї, бойових і забезпечуючих систем військового призначення;

деградації системи розробки озброєнь і військової техніки унаслідок складної економічної обстановки;

зміни кооперації розробників стратегічних оборонних систем і відчуження певної частини розробників до складу суміжних незалежних держав;

збільшення числа осіб та організацій, які можуть володіти інформаційною зброєю (включаючи терористичні групи);

слабкого розвитку науково-теоретичної бази з проблеми безпеки програмного забезпечення систем критичного застосування;

створення глобальних мережевих структур або підключення до них систем озброєння.

Порушення нормального функціонування інформаційних систем може викликати своєрідну "ланцюгову" реакцію негативних наслідків, що ще більше загострює проблему безпеки інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Ленков С.В.* Методы и средства защиты информации / С.В. Ленков, Д.О. Перегудов, В.А. Хорошко. – К. : Арий, 2008. – С. 163–180.

2. *Ярочкин В.И.* Информационная безопасность / В.И. Ярочкин. – М. : Международные отношения, 2000. – 400 с.

3. *Азаров С.С.* Современные модели провайдинга / С.С. Азаров, В.А. Хорошко. – К. : ПолиграфКонсалтинг, 2006. – 98 с.

4. Введение в криптографию / Под общей ред. В.В. Ященко. – С-Пб. : Питер, 2001. – 288 с.

5. *Онучин С.В.* Устройства защиты информации. Критерии выбора / С.В. Онучин // Connect! Мир связи. – 1998. – № 11. – С. 104.

6. [Електронний ресурс]. – Режим доступу : http://it2b.ru/.

7. [Електронний ресурс]. – Режим доступу : http://kiev-security.org.ua.

Отримано 03.04.2014