ЦИТ: 315-172
УДК 004.380

Фенко О.Г., Лисенко Д.І.

ПРОБЛЕМИ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, пр-т. Першотравневий 24, 36011

Fenko O.G., Lysenko D.I.

PROBLEMS OF SAFETY OF SOFTWARE

Poltava National Technical University named after Yuri Kondratyuk, Poltava, Ave. Pershotravnevuy 24, 36011

Анотація. У роботі проаналізовані міжнародні документи та норми з захисту інформації. Приведені приклади типових загроз інформаційним ресурсам. Проведений аналіз моделі сучасної технології шкідливих програм та забезпечення захисту на прикладі API та DLL-функцій операційної ситеми (ОС).

Ключові слова: інформаційна безпека, сучасні технології шкідливого програмного забезпечення (ПЗ)

Abstract. In-process analysed the international documents and norms from protection of the information. The resulted examples of typical threats for information resources the analysis of model of modern technology harmful programs and maintenance of protection Is lead by the example of API-functions and DLL-functions operational system (OS).

Key words: information safety, modern harmful technologies software

Вступ.

Безпека інформаційних технологій (ІТ) являє собою концепцію актуальних проблем комп'ютеризації держави. Її рішення визначається, у першу чергу, наявністю законодавчих актів і нормативно-технічних документів по забезпеченню безпеки ІТ.

Огляд літератури.

В даний час широко поширені мови програмування, такі как Java, у яких виконується, не машинний код, а машинно-нейтральне представлення. Задача декомпіляції програми з такого представения назад у програму мовою Java значно простіше, ніж декомпіляція з машинного коду. Одним зі способів боротьби з цим є заплутування програм (обфускація) [5,4]. Країною з розвинутою системою захисту інформаціїйного простору є США. Американці перші, хто зрозумів вислів про володіння інформацією, оскільки вони одними з перших у світі запровадили систему захисту інформації на законодавчому рівні. Зазначимо, що законодавство у напрямку захисту інформації цієї країни, перш за все, визначає об'єкти правової охорони в інформаційній сфері, порядок реалізації права власності на інформаційні об'єкти, права і обов'язки власників, правовий режим функціонування інформаційних технологій; категорії доступу окремих суб'єктів до певних видів інформацій, встановлює категорії секретності, поняття «конфіденційної інформації» та межі його правового застосування [1]. Разом із тим, слід наголосити, що інформація в США може

бути захищена за допомогою правових засобів захисту інтелектуальної власності. Зазначимо, що в США існують чотири основних закони з приводу інтелектуальної власності: закон про авторське право, патентний закон, закон про торгову марку, закон про торговий секрет. Особливий інтерес з приводу з'ясування питань регулювання інформаційних відносин становлять рішення саме щодо права власності та інтелектуальної власності на інформацію. Згідно законодавства США існує два види комерційної таємниці — це технологічна інформація та ділова інформація. Слід зазначити, що персональна інформація, у Сполучених Штатах розглядається відповідно до концепції «privacy». Ця концепція реалізується через „Стандарт CSA". Цей нормативно-правовий документ використовується в Америці головним чином тому, що поширюється на всі країни - члени НАТО [2]. Країни - учасники Європейського Союзу мають у певному сенсі злагоджену систему захисту інформації, але в той же час вона є розгалуженою, тому що, як зазначалося вище, хоча існує Директива щодо Захисту особистості з дотриманням режиму персональних даних і вільного руху таких даних, яка в принципі врегульовує певні питання, але при цьому майже кожна країна ЄС має свої закони, положення, інструкції, щодо врегулювання питань безпеки інформації. Така система має і свої переваги, та свої недоліки. Недолік полягає у тому, що обмін інформацією між країнами ускладнюється через певні неспівпадання у нормативних актах країн, про що було зазначено вище. Така ж проблема існує й у відносинах ЄС і України, оскільки інформаційне законодавство взагалі не співпадає з визначеннями понять у законодавстві Європейського Союзу [3].

Основний текст.

Оцінка безпеки інформаційних технологій і продуктів IT базується на критеріях безпеки комп'ютерних систем, приведених в основних документах. Основними документами в області оцінки безпеки IT є:

1. Федеральні критерії інформаційних технологій
2. "Помаранчева книга" (TCSEC)

Існує ряд міжнародних стандартів, що намагаються вирішити цю проблему, однак аж до останнього часу вони не могли претендувати на те, щоб стати керуючим документом до дії чи хоча б закласти фундамент безпечних інформаційних технологій майбутнього. У різних країнах, у тому числі і в Україні, розроблені документи, що являють собою лише деяке наслідування закордонним стандартам десятилітньої давнини. В умовах повальної інформатизації і комп'ютеризації найважливіших сфер державного апарата країні просто необхідні нові рішення в цій області.

В останні роки у світі різко загострилися проблеми, що пов'язані з забезпеченням безпечної діяльності людей узагалі. В умовах політичної та економічної нестабільності у світі зараз постійно виникають різні негативні явища від локальних війн до міжнародного тероризму.

Забезпечення безпеки виявилося прямо пов'язаним з інформаційною безпекою в наслідок широкого використання інформаційних технологій практично в усіх областях людської діяльності.

Оскільки комп'ютерні системи тепер прямо інтегровані в інформаційні

структури сучасного суспільства, засоби захисту повинні враховувати сучасні форми представлення інформації Це означає, що системи захисту повинні забезпечувати безпеку на рівні інформаційних ресурсів, а не окремих документів, файлів чи повідомлень.

Цю задачу потрібно вирішити в глобальному масштабі, незважаючи на те, що сторони, які беруть участь, можуть знаходитися в різних частинах планети, функціонувати на різних апаратних платформах і в різних ОС.

Досвід експлуатації існуючих систем показав, що сьогодні від систем захисту вимагаються зовсім нові функції, а саме, можливість забезпечення безпеки в умовах будь-якої їх взаємодії з подібними засобами, в тому числі і при появі усередині їх програм, що здійснюють деструктивні дії – комп'ютерних вірусів, автоматизованих засобів зламу, агресивних агентів. На перший погляд здається, що ця проблема вирішується засобами розмежування доступу, однак це не зовсім так, що підтверджується відомими випадками поширення комп'ютерних вірусів у «захищених» системах. Інтеграція захисту інформації в процес автоматизації її обробки, є обов'язковим елементом. Для того, щоб бути затребуваними сучасним ринком інформаційних систем, засоби безпеки не повинні істотно погіршувати характеристики існуючих застосувань і сформованих технологій обробки інформації, а навпаки, повинні стати невід'ємною частиною цих засобів і технологій.

Країни-учасники Європейського Союзу мають у певному сенсі злагоджену систему захисту інформації, але в той же час вона є розгалуженою, тому що, як зазначалося вище, хоча існує Директива щодо Захисту особистості з дотриманням режиму персональних даних і вільного руху таких даних, яка в принципі врегульовує певні питання, але при цьому майже кожна країна ЄС має свої закони, положення, інструкції, щодо врегулювання питань безпеки інформації. Така система має і свої переваги, та свої недоліки. Недолік полягає у тому, що обмін інформацією між країнами ускладнюється через певні неспівпадання у нормативних актах країн, про що було зазначено вище. Така ж проблема існує й у відносинах ЄС і України, оскільки інформаційне законодавство взагалі не співпадає з визначеннями понять у законодавстві Європейського Союзу.

Для України питання інформаційної війни актуальне, як ніколи і програмне забезпечення може завдати непоправної шкоди не тільки інформаційному простору, але і безпеці України, тому захист програмного продукту, його “правильність” дуже важлива. В теперишній час стало очевидним, що діяльність по захисту інформації і забезпеченню інформаційної безпеки є однієї з найважливіших задач забезпечення суверенітету й обороноздатності України. Інформаційний простір стає територією інформаційних воєн (наприклад повязаних з подіями на сході і в Криму), що дають можливість створення засобів небезпечного впливу на інформаційні сфери, порушення нормального функціонування інформаційних і телекомунікаційних систем, а також одержання несанкціонованого доступу до них.

Основною проблемою при захисті й оцінці уразливих місць в операційних

системах є контроль доступу, що реалізується на рівні користувача. У залежності від задач, які потрібно вирішувати за допомогою обчислювальної системи, обирається тип контролю доступу, що буде введений в інформаційну систему. Помилка в питанні поділу прав між користувачами може привести до витоку цінної інформації або її повної втрати. Технологія керування системою інформаційної безпеки держави формує таку систему інформаційної безпеки, що дозволить гарантовано забезпечити захист і безпеку, якщо буде існувати реальна загроза національній безпеці України. Технологія керування інформаційною безпекою заснована на загальному підході, призначена для розробки, упровадження, функціонування, моніторингу, перегляду, підтримки й удосконалювання інформаційної безпеки.

Прагнення нашої країни до високого рівню інформатизації, породжує проблему інформаційної безпеки. Ця проблема атуальна для усього світу, що йде по шляху інтеграції. Слід зазначити проблему вільного програмного забезпечення Обов'язковою вимогою повинні стати верифікація і сертифікація прийнятих продуктів за допомогою спеціалізованих програм, які варто закупити. Спочатку вихідний код аналізується статично, потім динамічно в робочому режимі з повним перебором вхідних параметрів у різних робочих умовах (варіація обсягу оперативної та віртуальної пам'яті і т.п.). При виявленні вразливостей і помилок у кодах, програми передаються розроблювачеві на доробку. Після цього програма надходить на повторне тестування. В широкому сенсі під надійністю програмного забезпечення розуміють його здатність функціонувати без прояву будь-яких негативних наслідків для конкретної комп'ютерної системи та її користувача. Одним із таких негативних наслідків є порушення цілісності та конфіденційності інформації в програмних комплексах комп’ютерних систем або надання програмним забезпеченням функціонально непридатних результатів обробки інформації. Серед причин цього, окрім різноманітних збоїв апаратури комп’ютерних систем, особливо слід відзначитиз збої, пов’язані з діями людей, які можна розділитина на дві категорії: навмисні і ненавмисні дії.

Базовою характеристикою інформаційної безпеки варто вважати імовірність появи і реалізації погроз підвищеного ризику або небезпеки для суспільства і держави.

Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушенням безпечного функціонуванням системи інформаційної безпеки.

Заключення та висновки.

Відзначаючи високий рівень активності і зацікавленості міжнародного співтовариства у стратегічному вирішенні проблем розвитку інформаційного простору, розглянуте визначення інформаційної безпеки, яке є комплексним і досвід провідних країн у цій сфері, який може стати прикладом для України у формуванні її власної стратегії в інформаційному середовищі.

Література:

1. Беляков К. Інформація організаційно-правової сфери /К.Беляков // Право

України. —2004. —№ 6. — С. 88-92.

2. Климчук С. Загальна характеристика законодавства про інформаційну безпеку ЄС, США та Канади / С.Климчук // Юстініан, 2006. — № 11. — ГУМАНІТАРНІ НАУКИ Вісник КДУ імені Михайла Остроградського.

3. Климчук С. Проведення порівняльного аналізу законодавства у сфері інформації з обмеженим доступом України та країн-членів НАТО / С.Климчук //Юстиніан, 2007. — №4..

4. Класифікація автоматизованих систем і стандартні функціональніпрофілі захищеності оброблюваної інформації від несанкціонованого доступу:НД ТЗІ 2.2–005–99. – Київ: ДСТСЗІ СБ України, 1999. – 23 с.).

5. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – Київ: ДСТСЗІ СБ України,1999. – 26 с..

Стаття відправлена: 28.09.2015р.

ЦИТ: 315-144
УДК 004.735

Акимов С.В., Верхова Г.В.

ВИРТУАЛЬНАЯ УЧЕБНАЯ ЛАБОРАТОРИЯ

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ),
Санкт-Петербург, Проспект Большевиков 22-1, 193232

Akimov S.V., Verkhova G.V.

VIRTUAL EDUCATIONAL LABORATORY

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Saint-Petersburg, Prospekt Bolshevikov 22-1, 193232

Аннотация. В работе рассматривается виртуальная учебная лаборатория, обеспечивающая поддержку проведения лабораторных работ как в режиме аудиторных занятий, так и при дистанционном обучении. Рассматриваемая виртуальная учебная лаборатория призвана обеспечить переход от традиционных учебно-методических комплексов к мультимедийным, а также внедрение в образовательный процесс технологии виртуальных предприятий. Виртуальная учебная лаборатория предполагает глубокую интеграцию в формирующееся в настоящее время единое академическое информационное пространство. Внедрение виртуальной учебной лаборатории повысит эффективность работы преподавателей, будет способствовать усилению мотивации студентов и приобретению ими навыков работы с технологиями виртуальных предприятий и производств, обеспечит обмен опытом и материалами, входящими в мультимедийные учебно-методические комплексы, сократит объем расходных материалов, необходимых для подготовки отчетов студентов по выполнению лабораторных работ.