УДК 681.3

ІНФОРМАЦІЙНА БЕЗПЕКА В КОМП'ЮТЕРНИХ ПРОГРАМАХ ТА СИСТЕМАХ

Фурман І. О., Старовєров Р. М., Піскарьов О. М.

Харківський національний технічний університет сільського господарства імені Петра Василенка

Наведено огляд сучасних методів і засобів інформаційної безпеки в комп'ютерних програмах та системах.

Постановка проблеми. У сучасному світі, що швидко змінюється, проблема інформаційної безпеки є однією з ключових складових діяльності будь-якого підприємства - чим складніша й розгалужена інформаційна система, тим важче її вирішити. Досить часто підприємства, придбавши велику кількість різних засобів захисту, стикаються з цілим рядом проблем. Річ у тому, що вони вимушені вирішувати комплексну і досить складну задачу: захищатися від постійно зростаючої кількості загроз, і одночасно з цим розгортати закуплені засоби забезпечення безпеки та керувати ними.

Найголовніша проблема - нестача кваліфікованих фахівців в цій області й відсутність у наявних IT - спеціалістів необхідних знань і практичного досвіду по організації інформаційної безпеки в умовах різнорідного інформаційного середовища, оскільки вже наявні в штаті співробітники найчастіше переобтяжені і вимушені одночасно вирішувати як організаційні, так й технічні завдання.

Аналіз останніх досліджень та публікацій. Ключовими аспектами вирішення проблеми інформаційної безпеки комп'ютерних систем є розробка вимог, критеріїв (показників) і відповідних методик оцінки рівня інформаційної безпеки.

Необхідно відмітити, що оцінка інформаційної безпеки комп'ютерних систем (КС) повинна проводитися в три етапи:

- оцінка технології, що впроваджується в КС, з точки зору інформаційної безпеки;
- сертифікація апаратно-програмного комплексу, що впроваджується в КС за вимогами безпеки інформації;
- аудит інформаційної безпеки КС з метою перевірки відповідності досягнутого рівня цієї безпеки, вказаному в технічному завданні на їх розробку.

Мета статті. У цих умовах виникає вразливість КС двох видів: з одного боку, можливість знищення або спотворення інформації (тобто порушення її фізичної цілісності), а з іншої - можливість несанкціонованого використання інформації (тобто небезпека просочування інформації обмеженого користування). Метою даної статті є розгляд вразливості першого типу.

Основні матеріали дослідження. В наш час проблеми, пов'язані із захистом інформації непокоять як фахівців в області комп'ютерної безпеки так і багаточисельних рядових користувачів персональних комп'ютерів. Це пов'язано з глибокими змінами, що вносяться комп'ютерною технологією в наше життя.

Змінився сам підхід до поняття "інформації". Цей термін зараз більше використовується для позначення спеціального товару який можна купити, продати, обміняти на щось інше і так далі. При цьому вартість подібного товару часто перевершує в десятки, а то і в сотні разів вартість самої комп'ютерної техніки, в рамках якої він функціонує.

Захистом інформації називають діяльність по запобіганню витоку інформації, несанкціонованих і неумисних дій на інформацію, що захищається.

Під неумисною дією на інформацію, що захищається, розуміють дію на неї із-за помилок користувача, збою технічних або програмних засобів, природних явищ, інших нецілеспрямованих дій (наприклад, знищення документів в результаті відмови носія інформації - накопичувача на жорсткому магнітному диску, флеш пам'яті або інше).

Загрози інформаційної безпеки можуть бути розділені на загрози, які не залежать від діяльності людини (природні загрози фізичних дій на інформацію стихійних природних явищ), і загрози, викликані людською діяльністю (штучні загрози), які є набагато небезпечнішими.

Штучні загрози виходячи з їх мотивів розділяються на неумисні (випадкові) і умисні.

До неумисних загроз відносяться:

- помилки в проектуванні КС;
- помилки в розробці програмних засобів КС;
- випадкові збої в роботі апаратних засобів КС, ліній зв'язку, енергопостачання;
- помилки користувачів КС;
- дія на апаратні засоби КС фізичних полів інших електронних облаштувань (при недотриманні умов їх електромагнітної сумісності) та ін.

Природно, виникає потреба захистити інформацію як від несанкціонованого доступу, крадіжки, знищення і інших злочинних дій, так і від дій, які не мали на меті злочинного наміру. Велика частина користувачів не усвідомлює, що постійно ризикує своїми даними, відносячись не професійно до роботи на комп'ютері. Користувачі комп'ютерних систем по необачності можуть знищувати навіть такі дані як податкова та банківська інформація, ділове листування й електронні таблиці.

Останніми роками у сфері зв'язку і інформатизації здійснюється велика робота з модернізації існуючих та побудови сучасних КС. Різноманіття КС ставить ряд проблем, серед яких однією з найважливіших є проблема координації створення і розвитку захищених КС. Спроби розв'язати проблему інформаційної безпеки виключно криптографічними методами не забезпечує належного результату, тому нині у сфері зв'язку і інформатизації встає проблема забезпечення не лише конфіденційності інформації, але і забезпечення цілісності самої інфраструктури і інформації, а також доступності інформаційних ресурсів і послуг.

Вміст проблеми захисту інформації фахівцями інтерпретуються таким чином. В міру розвитку і ускладнення засобів, методів і форм автоматизації процесів обробки інформації підвищується її уразливість. Основними чинниками, сприяючими підвищенню цієї уразливості, є:

- різке збільшення об'ємів інформації, що нагромаджується, зберігається і оброблюваної за допомогою КС та інших засобів автоматизації;
- різке розширення кола користувачів, що мають безпосередній доступ до ресурсів КС та даних, що знаходяться в ній;
- ускладнення режимів функціонування технічних засобів КС.

Використовувані нині на практиці підходи до забезпечення інформаційної безпеки КС повинні визначатися наступними етапами:

- вимогами до інформаційної безпеки, системами забезпечення інформаційної безпеки, що реалізовуються, та регламентуючими відповідними нормативними документами в області інформаційної безпеки;
- реальними послугами і механізмами захисту, що реалізуються в системах забезпечення інформаційної безпеки;
- існуючою статистикою загроз безпеки для конкретної мережі телекомунікації, потенційно можливими загрозами, а також причинами вразливостей.

Оцінка інформаційної безпеки КС повинна проводитися з метою перевірки відповідності досягнутого рівня інформаційної безпеки заданому рівню при проектуванні КС. Оцінка інформаційної безпеки КС є також важливим засобом забезпечення гарантованості реалізації вибраних механізмів, методів і засобів інформаційної безпеки.

В умовах динамічного розвитку КС і виникнення нових загроз інформаційної безпеки важливим стає аналіз і управління ризиками інформаційної безпеки. Аналіз ризиків полягає в тому, щоб виявити існуючі риски інформаційної безпеки і оцінити їх величину (дати їм якісну або кількісну оцінку). Управління рисками інформаційної безпеки пов'язане із вжиттям заходів забезпечення інформаційної безпеки, спрямованих на зниження частоти реалізації загроз і розміру збитку у разі їх реалізації.

Міжнародний досвід розвинених країн показує, що об'єктивною і незалежною оцінкою відповідності систем і засобів забезпечення інформаційної безпеки встановленим вимогам безпеки являється сертифікація систем і засобів на відповідність вимогам безпеки інформації. Найбільш важливими нормативно-правовими документами при створенні і розвитку захищених КС є документи, що стандартизують вимоги, показники і критерії оцінки безпеки. До числа найважливіших завдань в області забезпечення інформаційної безпеки КС відносяться:

- аналіз і розробка вимог, показників, критеріїв і методів оцінки ефективності систем і засобів забезпечення інформаційної безпеки;
- сертифікація систем і засобів забезпечення інформаційної безпеки на основі сучасних вимог.

Для проведення сертифікації за вимогами безпеки інформації потрібна наявність критеріїв оцінки, якими виступає набір вимог безпеки, сформульованих у відповідних національних і міжнародних стандартах.

Висновки. В цілях ефективного рішення вищерозглянутих завдань потрібне створення національної системи сертифікації систем і засобів забезпечення інформаційної безпеки за вимогами безпеки інформації, розробка методичних основ їх сертифікації на основі загальних критеріїв.

Основні висновки по аналізу інформаційної безпеки КС зводяться до наступного:

- найбільший ефект досягається тоді, коли всі засоби, методи і заходи об'єднуються в єдиний, цілісний механізм захисту інформації;
- механізм захисту повинен проектуватися паралельно із створенням систем обробки даних, починаючи з моменту вироблення загального задуму побудови системи;
- функціонування механізму захисту повинне плануватися і забезпечуватися разом з плануванням і забезпеченням основних процесів автоматизованої обробки інформації;
- необхідно здійснювати постійний контроль функціонування механізму захисту.

Список використаних джерел

1. Хорев П. Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / М.: Издательский центр "Академия", 2005. — 256 с
2. Фурман І. О. Заходи з захисту комп’ютерних програм та систем від ненавмисних дій користувачів / І. О. Фурман, Р. М. Старовєров // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Технічні науки – Харків: ХНТУСГ, 2009. – Вип. 89. – С. 95-96.
3. Український ресурс з безпеки. – [Електроний ресурс]: http://www.kiev-security.org.ua
4. Борисов М. А. Основы программно-аппаратной защиты информации. / М. А. Борисов, И. В. Заводцев, И. В. Чижов. - М.: Книжный дом "ЛИБРОКОМ", 2013. — 376 с.

Аннотация

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ ПРОГРАММАХ И СИСТЕМАХ

Фурман И. А., Староверов Р. Н., Пискарев А. Н.

Приведен обзор современных методов и средств информационной безопасности в компьютерных программах и системах.

Abstract

INFORMATION SECURITY THE COMPUTER PROGRAM AND SYSTEMS

I. Furman, R. Staroverov, A. Piskarev

The review of modern methods and means of information security in computer programs and systems.