моделювання. Існує клас об'єктів, для яких з різних причин не розроблені аналітичні моделі або не розроблені методи вирішення отриманої моделі. В цьому випадку математична модель замінюється імітатором або імітаційною моделлю.

Імітаційна модель – логіко-математичний опис об'єкта, який може бути використаний для експериментування на комп'ютері в цілях проектування, аналізу та оцінки функціонування об'єкта. Як приклад виступає проведення краш-тестів. Краш-тест – випробування дорожніх і гоночних автомобілів на безпеку. Є умисним відтворенням дорожньо-транспортної події з метою з'ясування рівня пошкоджень, які можуть отримати його учасники.

Діагностика транспортних засобів відіграє важливу роль у відновленні автомобільного парку і проведенні профілактичних мір, що гарантують безпеку руху та визначають екологічний вплив автотранспорту на навколишнє середовище. Для підтримання рухомого складу в технічно справному стані необхідно розширювати систему діагностування з використанням сучасних інформаційних систем та проводити необхідні попереджувальні ремонтні роботи.

Список використаних джерел:

1. Надежность и эффективность в технике. Справочник в десяти томах / В. С. Абдуевский; под. общ. ред. В. В. Клюева. М. : Машиностроение. Т.9. – Техническая діагностика; под. общ. ред. В. В. Клюева. – 352 с.
2. Дейнеко Т. О. Інформаційний бізнес як інноваційний засіб розвитку економіки України / Т. О. Дейнеко. – Львів , 2002. – 286 с.

Франко Ю. П., ТНПУ ім. В. Гнатюка
(м. Тернопіль)

ВИВЧЕННЯ СТУДЕНТАМИ КОМП'ЮТЕРНОГО ПРОФІЛЮ ІНЖЕНЕРНО-ПЕДАГОГІЧНИХ ФАКУЛЬТЕТІВ ПРИНЦИПІВ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

Комп'ютерні технології все стрімкішими темпами входять в усі сфери життя суспільства, що викликає потребу підготовки фахівців різних напрямів, у тому числі інженерів-педагогів комп'ютерного профілю.

Інформаційні ресурси в сучасних умовах є одним із найважливіших результатів діяльності людського суспільства. Саме тому особлива увага приділяється задачі захисту інформації. Особливого рівня актуальності набуває ця задача в умовах стрімкого розвитку сучасних інформаційних технологій. Такі технології з кожним роком залучають все більшу частину інформаційних ресурсів у процес електронної обробки, що в свою чергу спричиняє зріст вимог щодо параметрів програмно-апаратних засобів, які використовуються для захисту. З іншого боку, розвиваються нові системи захисту, побудовані на традиційних підходах. Збільшується кількість та різнорідність кінцевих користувачів, що залучаються до обробки інформаційних ресурсів. У процесі обробки інформації використовуються розподілені, неоднорідні комп'ютерні системи та мережі, політика безпеки яких суттєво відрізняється одна від одної. Усі ці аспекти створюють нові

передумови щодо розробки методів та засобів захисту інформаційних ресурсів від цілої гами різноманітних загроз.

Розвиток нових інформаційних технологій, загальна комп'ютеризація та різке збільшення кількості комп'ютерних систем і мереж (КСМ) призвели до того, що інформаційна безпека не тільки стає обов'язковою, вона ще й одна з характеристик інформаційних систем. Фактор безпеки інформаційних ресурсів і послуг при розробці та експлуатації сучасних КСМ відіграє першорядну роль. Під час організації систем захисту потрібно керуватися рядом принципів, які забезпечать якісний захист та протидію від наявних загроз.

Проблема захисту інформації шляхом її перетворення, що унеможливлює прочитання цієї інформації сторонньою особою, ще декілька десятиліть тому стосувалася в основному військових операцій. Бурхливе використання комп'ютерних мереж та поява нових потужних обчислювальних засобів спричинили швидкий розвиток криптографії.

Ціль захисту інформації в КСМ є процес протидії впливу на інформаційні ресурси та послуги, якщо цей вплив виконується з метою порушення конфіденційності, цілісності та доступності, а саме знищення, крадіжка, зниження ефективності функціонування або несанкціонований доступ.

Мета статті – аналіз та класифікація актуальних загроз інформаційним ресурсам сучасних КСМ, а також задача досліджень – визначення, на основі проведеного аналізу, основних принципів організації захисту.

Класифікація загроз інформаційним ресурсам. Побудова надійного та ефективного захисту інформаційної системи неможлива без попереднього аналізу можливих загроз безпеки системи. Цей аналіз повинен складатися з таких етапів :

- виявлення характеру інформації, яка зберігається в системі;
- оцінка цінності інформації, яка зберігається в системі;
- побудова моделі зловмисника;
- визначення та класифікація загроз інформації в системі (несанкціоноване зчитування, несанкціонована модифікація і т. д.);

Під загрозою безпеки інформаційним ресурсам розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів [1–3].

Загрози інформаційним ресурсам та послугам можна класифікувати за такими критеріями (рис.1):

- інформаційної безпеки (загрози конфіденційності даних і програм; загрози цілісності даних, програм, апаратури; загрози доступності даних; загрози відмови від виконання операцій);
- за компонентами інформаційних систем, на які загрози спрямовані (інформаційні ресурси та послуги, персональні дані, програмні засоби, апаратні засоби, програмно-апаратні засоби);

- за способом здійснення (випадкові, навмисні, дії природного та техногенного характеру);

- за розташуванням джерела загроз (внутрішні та зовнішні).

Рис.1 Класифікація базових загроз інформаційних ресурсів та послуг в сучасних комп'ютерних системах та мережах

Всі загрози безпеки, спрямовані проти програмних і технічних засобів інформаційної системи, впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей інформації, яка зберігається і обробляється в інформаційній системі. Як правило, загрози інформаційній безпеці розрізняються за способом їх реалізації.

Дослідження й аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на випадкові і навмисні.

Якщо розглядати класичну систему організації впливу на КСМ, то всі загрози поділяються на випадкові, чи ненавмисні та навмисні. Джерелом ненавмисних загроз інформаційних систем можуть бути вихід з ладу апаратних чи програмних засобів, неправильні дії працівників або її користувачів, ненавмисні помилки в програмному та програмно-апаратному забезпеченні і т. д. Такі загрози можуть нанести значний збиток. Однак більш значними з точки зору ефективності функціонування КСМ є навмисні загрози, які, на відміну від випадкових, мають на меті завдання збитків інформаційній системі або користувачам. Навмисні загрози можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами тощо. Наслідки такі: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути досить високою [2, 3].

Для вирішення поставленої задачі і створення ефективної системи безпеки інформації, розроблення та вдосконалення існуючих методів

захисту доцільно навести найбільш повну класифікацію загроз і шляхів їх реалізації в КСМ.

Можна виділити актуальні загрози безпеці, які спрямовані проти інформаційних ресурсів у сучасних інформаційно-комунікаційних системах та мережах:

- протиправне збирання і використання інформації;
- порушення технології обробки інформації;
- впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби;
- розробка і поширення програм, що порушують нормальне функціонування інформаційних та інформаційно-телекомунікаційних систем, у тому числі систем захисту інформації;
- радіоелектронний вплив з метою виведення з ладу, пошкодження чи руйнування засобів і систем обробки інформації, телекомунікації зв’язку;
- вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації;
- витік інформації технічними каналами;
- впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, зберігання і передачі інформації з каналів зв'язку, а також у службові приміщення органів державної влади, підприємств, установ та організацій усіх форм власності;
- знищення, пошкодження, руйнування чи розкрадання машинних та інших носіїв інформації;
- перехоплення інформації в мережах передачі даних та лініях зв’язку, дешифрування цієї інформації і нав’язування хибної інформації;
- використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації зв'язку при створенні і розвитку інформаційної інфраструктури України;
- несанкціонований доступ до інформації, що знаходиться в банках і базах даних;
- порушення законних обмежень на поширення інформації.

Основні принципи організації захисту інформаційних систем. Під час організації ефективного та надійного захисту потрібно керуватися системою принципів. Під принципами захисту інформації розуміються основні ідеї і найважливіші рекомендації з питань організації та здійснення робіт для ефективного захисту інформаційних ресурсів КСМ. Використання таких принципів дозволяє ефективно організувати роботу з захисту інформації.

Загалом принципи захисту інформації можна умовно розділити на дві основні групи:

- правові принципи;
- організаційні принципи.

Правові принципи захисту інформації

Правове регулювання захисту інформації спирається на принципи

інформаційного права. Ці принципи, що базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, а також гарантують їх здійснення.

Крім того, основні правові засади захисту інформації ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об'єкта правовідносин.

Узагальнено до правових принципів захисту інформації відносяться: легітимність (законність); пріоритет міжнародного права над внутрішньодержавним; економічна доцільність.

Організаційні принципи захисту даних

Роль організаційного захисту інформації в системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів.

Організаційні методи захисту передбачають проведення організаційно-технічних та організаційно-правових заходів, а також включають такі принципи захисту інформації:

- науковий підхід до організації захисту інформації;
- планування захисту;
- керування системою захисту;
- безперервність процесу захисту інформації;
-мінімальна достатність організації захисту;
- системний підхід до організації та проектування систем та методів захисту інформації;
- комплексний підхід до організації захисту інформації;
- відповідність рівня захисту цінності інформації;
- гнучкість захисту;
- багатозональність захисту, що передбачає розміщення джерел інформації в зонах із контрольованим рівнем її безпеки;
- багаторубіжність захисту інформації;
- обмеження числа осіб, які допускаються до захищеної інформації;
- особиста відповідальність персоналу за збереження довіреної інформації.

Висновок

Таким чином, на основі проведеного аналізу сучасних загроз інформаційним ресурсам систем та мереж передачі даних проведено їх класифікацію за базовими критеріями. На основі проведених досліджень запропоновано систему принципів організації захисту інформаційних систем.

Список використаних джерел:

1. Мельников В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. – М.: Финансы и статистика, 2003. – 368 с.
2. Малюк А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк, С. В. Пазизин, Н. С. Погожин :[учеб. пособие] . – М.: Горячая линия - Телеком, 2005. – 147 с.

3. Юдін О. К. Захист інформації в мережах передачі даних / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. :[підручник]. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.
4. Ярочкин В. И. Информационная безопасность / В. И. Ярочкин. – [учебник для вузов]. 4-е издание. Серия: Gaudeamus. – М.: Академический проект, 2006. – 544 с.

Цідило І. М. , ТНПУ ім. В. Гнатюка
(м. Тернопіль)

ДО ПРОБЛЕМИ ЗАСТОСУВАННЯ ЗНАНЬ НА ПРАКТИЦІ

Традиційно процес засвоєння в дидактиці описується ланцюжком: сприйняття, розуміння, осмислення, узагальнення, закріплення, застосування. Усе це так. Але остання ланка цього ланцюжка повністю називається «Застосування отриманих знань на практиці». Але про яку практику йде мова?! Під цим «застосуванням» є, зважаючи лише на виконання вправ, рішення «завдань» (у сенсі прикладів, вправ і т. д.) із того ж навчального курсу – якщо вивчається математика – це рішення прикладів із математики і так далі – «не виходячи» за рамки курсу. Це «застосування на практиці» є настільки академічним, що до справжнього життя, до дійсної практики, практичної діяльності людей в більшості випадків не має відношення.

У теоретичних роботах із дидактики та педагогічної психології проблема застосування знань розглядалася в основному так, що в процесі рішення завдань, у тому числі «практичних», учень (студент) повинен проаналізувати умови, які в ній дані відкрито, в явному вигляді, і виділити (угледіти) ті приховані умови, опора на які і призводить до рішення задачі.

Між тим проблема застосування знань у практичній діяльності набагато складніша. Діяльність людини в новій ситуації, коли потрібне застосування готових знань, полягає в активному пізнанні самого об’єкта діяльності, в орієнтуванні, «поверненні» об’єкту з різних сторін, в «відпрацюванні» уявлень про нього, вичлененні предмета, мети і засобів власної діяльності, переформулюванні попередніх знань, співвідношенні їх з готовою ситуацією в різних площинах, в різних структурах відношень, на різних рівнях спілкування [3, с. 186].

У більшості реальних практичних ситуацій від учня (студента) потрібні аналіз із застосування у взаємозв'язку багатьох різнорідних понять, принципів, законів з різних розділів, різних галузей знань. Так, для грамотного вибору і використання токарного різця необхідно знати не лише властивість клину, який використовується в усіх різальних інструментах, але і умови теплопровідності, тепловіддачі різальних поверхонь, поняття про важіль, закони статики, властивості твердості