Науковий пошук молодих дослідників: збірник наукових праць / за ред. канд. пед. наук Королюк О.М. – Випуск 6. – Житомир: Вид-во ЖДУ ім. І.Франка, 2013. – С. 230-233.

Вакалюк Тетяна Анатоліївна,

старший викладач кафедри прикладної математики та інформатики

ОСНОВНІ ПОНЯТТЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ У КОМП'ЮТЕРНИХ СИСТЕМАХ

Зростання ролі й відповідальності інформаційних технологій у життєдіяльності людини неминуче спричиняє відповідальне відношення до забезпечення надійної, безпечної роботи автоматизованих комп'ютерних систем. Помилки у функціонуванні автоматизованих комп'ютерних систем можуть призвести до досить серйозних наслідків. Захищена від зовнішніх і внутрішніх загроз автоматизована комп'ютерна система – це те, до чого прагнуть керівники великих підприємств і власники домашніх персональних комп'ютерів. Захист інформаційних ресурсів – справа, необхідність і значимість якої продиктоване практикою. У цій справі одну з важливих ролей відіграють програмні засоби захисту інформаційних ресурів.

Інформаційні ресурси – це відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх подання. ***Інформаційними ресурсами*** називають документи і масиви документів, що існують окремо або в складі інформаційних систем. Залежно від форми подання інформаційні ресурси можуть бути розділені на мовні, телекомунікаційні та документовані.

Мовні інформаційні ресурси виникають в ході ведення в приміщеннях розмов, роботи систем зв'язку, звукопідсилення та звуковідтворення.

Телекомунікаційні інформаційні ресурси циркулюють в технічних засобах обробки і зберігання інформаційних ресурів, а також в каналах зв'язку при їх передачі.

До ***документованих інформаційних ресурсів*** (або документів) відносять інформаційні ресурси, представлені на матеріальних носіях разом з ідентифікуючими їх реквізитами.

До ***інформаційних процесів*** відносять процеси збору, обробки, накопичення, зберігання, пошуку і розповсюдження інформаційних ресурсів.

Під ***інформаційною системою*** розуміють впорядковану сукупність

документів і масивів документів та інформаційних технологій, що реалізують інформаційні процеси.

Інформаційні ресурси поділяються на: відкритого та обмеженого доступу. До обмеженого доступу належать: державна таємниця та конфіденційна інформація, яка, в свою чергу, поділяється на: службову таємницю (адвокатська таємниця, таємниця суду і слідства тощо); комерційну таємницю (банківська); персональні дані (відомості про факти, події і обставини життя громадянина, що дозволяють ідентифікувати його особу).

До інформаційних ресурсів, що захищаються відноситься такі, що є предметом власності і підлягають захисту відповідно до вимог правових документів або вимог, встановлених власником-розпорядником інформаційних ресурсів.

Захистом інформаційних ресурсів називають діяльність щодо запобігання витоку інформаційних ресурсів, несанкціонованих і ненавмисних дій на ці інформаційні ресурси.

Під ***витоком*** розуміють неконтрольоване поширення інформаційних ресурсів шляхом їх розголошення, несанкціонованого доступу до них та отримання розвідками. ***Розголошення*** – це доведення інформаційних ресурсів до неконтрольованої кількості одержувачів інформаційних ресурсів (наприклад, публікація відомостей на відкритому сайті в мережі Інтернет або у відкритій пресі). ***Несанкціонований доступ*** – отримання інформаційних ресурсів зацікавленим суб'єктом з порушенням правил доступу до них.

Несанкціонований вплив на інформаційні ресурси – вплив з порушенням правил їх зміни (наприклад, навмисне впровадження в інформаційні ресурси шкідливого програмного коду чи навмисна підміна електронного документу).

Під ***ненавмисним впливом*** на інформаційні ресурси розуміють вплив на них через помилки користувача, збій технічних чи програмних засобів, природних явищ, інших нецілеспрямованих впливів (наприклад, знищення документів у результаті відмови накопичувача на жорсткому магнітному диску комп'ютера).

Метою захисту інформаційних ресурсів є запобігання шкоди власнику-

розпоряднику, власнику чи користувачу інформаційних ресурсів. Під ефективністю захисту інформаційних ресурсів розуміють ступінь відповідності результатів захисту інформаційних ресурсів поставленій меті. Об'єктом захисту виступають інформаційні ресурси, їх носії або інформаційний процес, у відношенні яких необхідно забезпечувати захист у відповідності з поставленою метою.

Під якістю інформаційних ресурсів розуміють сукупність властивостей, що обумовлюють придатність інформаційних ресурсів задовольняти певні потреби їх користувачів відповідно до призначення інформаційних ресурсів. Одним з показників якості інформаційних ресурсів є їх захищеність – підтримання на заданому рівні тих параметрів інформаційних ресурсів, що характеризують встановлений статус їх зберігання, обробки та використання.

Основними характеристиками інформаційних ресурсів є:
1) конфіденційність інформаційних ресурсів – це відомість змісту тільки тим суб'єктам, які мають відповідні повноваження. Конфіденційність є суб'єктивною характеристикою інформаційних ресурсів, пов'язаною з об'єктивною необхідністю захисту законних інтересів одних суб'єктів від інших; 2) ***цілісність інформаційних ресурсів*** – це незмінність інформаційних ресурсів в умовах їх випадкового і (або) навмисного викривлення або руйнування; 3) ***доступність інформаційних ресурсів*** – це здатність забезпечення безперешкодного доступу суб'єктів до інформаційних ресурсів, що їх цікавить.

Сукупність інформаційних ресурсів та системи формування, розповсюдження і використання інформаційних ресурсів називають ***інформаційним середовищем суспільства.***

Під ***інформаційною безпекою*** розуміють стан захищеності інформаційного середовища, що забезпечує його формування та розвиток. Вона досягається шляхом реалізації політики безпеки.

Політика безпеки – це набір документованих норм, правил і практичних прийомів, що регулюють управління, захист і розподіл інформаційних ресуврсів обмеженого доступу.

Комп'ютерною системою (КС) обробки інформації називають організаційно-технічну систему, що включає в себе: технічні засоби обчислювальної техніки і зв'язку; методи та алгоритми обробки інформації, реалізовані у вигляді програмних засобів; інформацію (файли, бази даних) на різних носіях; обслуговуючий персонал та користувачів, об'єднаних за організаційно-структурними, тематичними, технологічними чи іншими ознаками.

Під ***програмними засобами захисту інформаційних ресурсів*** розуміють спеціальні програми, що включаються до складу програмного забезпечення КС виключно для виконання захисних функцій.

До основних програмних засобів (ПЗ) захисту інформаційних ресурсів належать: програми ідентифікації і аутентифікації користувачів КС; програми розмежування доступу користувачів до ресурсів КС; програми шифрування інформації; програми захисту інформаційних ресурсів від несанкціонованої зміни, використання та копіювання.

До переваг ПЗ захисту інформаційних ресурсів належать: простота тиражування; гнучкість; практично необмежені можливості їх розвитку шляхом внесення змін для урахування нових загроз безпеки інформаційних ресурсів.

До недоліків ПЗ захисту інформаційних ресурсів належать: зниження ефективності КС за рахунок споживання її ресурсів, необхідних для функціонування програм захисту; більш низька продуктивність; пристикованість багатьох ПЗ захисту, що створює для порушника принципову можливість їх обходу; можливість зловмисної зміни програмних засобів захисту в процесі експлуатації КС.

Список використаних джерел:

1. Мельников В. В. Защита информации в компьютерных системах /В. В. Мельников. – М. : Финансы и статистика; Электронинформ, 1997. – 368 с.