ОСОБЛИВОСТІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Палагнюк Д. М., Тищук Д. С. студенти IV курсу ФІРЕН; Березюк О. В., к.т.н., доцент
Вінницький національний технічний університет, м. Вінниця

Проблема інформаційної безпеки набула особливої значущості в сучасних умовах широкого застосування автоматизованих інформаційних систем, заснованих на використанні комп'ютерних і телекомунікаційних засобах [1]. При забезпеченні інформаційної безпеки стали цілком реальними загрози, викликані навмисними (зловмисними) діями людей. Перші повідомлення про факти несанкціонованого доступу до інформації були пов'язані, в основному, з хакерами, або «електронними розбійниками». Останнім десятиліттям порушення захисту інформації прогресує з використанням програмних засобів і через глобальну мережу Інтернет. Досить поширеною загрозою інформаційної безпеки стало також зараження комп'ютерних систем так званими вірусами.

Актуальність дослідження полягає в збільшенні і покращенні інформаційної безпеки та програмного забезпечення.

Інформаційна безпека (ІБ) – це стан захищеності інформаційного середовища, захист інформації являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається, тобто процес, спрямований на досягнення цього стану [2]. Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту.

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та мети тощо. При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку.

Загрози інформаційній безпеці – це можливі дії або події, які можуть вести до порушень ІБ. Види загроз інформаційній безпеці дуже різноманітні і мають безліч класифікацій. Загрози за видом об'єкта впливу вони поділяються на загрози власне інформації, загрози персоналу об'єкта та загрози діяльності щодо забезпечення інформаційної безпеки об'єкта. При більш детальному розгляді загроз інформації, їх можна поділити на загрози носіям конфіденційної інформації, місцям їх розміщення (розташування), каналам передачі (системам інформаційного обміну), а також інформації, що зберігається в документованому (електронному) вигляді на різних носіях.

При розробці необхідних, засобів, методів і заходів, що забезпечують захист інформації, необхідно враховувати велику кількість різних факторів.

Інформація, будучи предметом захисту, може бути представлена на різних технічних носіях. Її носіями можуть бути люди з числа користувачів і обслуговуючого персоналу. Інформація може піддаватися обробці в комп'ютерних системах, передаватися по каналах зв'язку і відображатися різними пристроями. Вона може розрізнятися за своєю цінністю. Об'єктами, що

підлягають захисту, де може перебувати інформація, є не тільки комп'ютери і канали зв'язку, але й приміщення, будівлі та прилегла територія. Істотно різнитися може кваліфікація порушників, а також використовувані способи і канали несанкціонованого доступу до інформації.

Прикладом застосування захисту інформації може слугувати захист криптостійкими алгоритмами файлів з тестовими запитаннями і варіантами відповідей, необхідних для проведення перевірки знань студентів шляхом комп'ютерного тестування [3-5].

Таким чином, основними принципами забезпечення інформаційної безпеки є такі [6]: системності, комплексності, безперервності захисту, розумної достатності, гнучкості управління і застосування, відкритості алгоритмів і механізмів захисту, простоти застосування захисних заходів і засобів.

За способами здійснення всі заходи забезпечення безпеки комп'ютерних систем поділяють на: правові (законодавчі), морально-етичні, організаційно-адміністративні, фізичні, апаратно-програмні.

Отже, в сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації, яка повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

Список літератури

1. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту // Ефективна економіка [Електронне наукове фахове видання]. – 2014. – № 5. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=3304.

2. Кавун С.В., Носов В.В., Мажай О.В. Інформаційна безпека: навчальний посібник. Ч. 1. – Харків: Вид. ХНЕУ, 2008. – 352 с.

3. Березюк О.В., Лемешев М.С., Віштак І.В. Комп'ютерна програма для тестової перевірки рівня знань студентів // Тезиси наук.-техн. конф. студентів, магістрів та аспірантів «Інформатика, управління та штучний інтелект», 26-27 листопада 2014 р. – Харків: НТУ «ХПІ», 2014. – С. 7.

4. Березюк О.В., Лемешев М.С., Томчук М.А. Перспективи тестової комп'ютерної перевірки знань студентів із дисципліни "Безпека життєдіяльності" // Матер. 9-ї міжнар. наук.-метод. конф. "Безпека життя і діяльності людини – освіта, наука, практика". – Львів, 2010. – С. 217-218.

5. Березюк Л.Л., Березюк О.В. Тестова комп'ютерна перевірка знань студентів із дисципліни «Медична підготовка» // Науково-методичні орієнтири професійного розвитку особистості: тези доповідей учасників IV Всеукраїнської науково-методичної конференції, 20.04.2016. – Вінниця: ТОВ «Меркьюрі – Поділля», 2016. – С. 96-98.

6. Аникин И.В., Глова В.И., Нейман Л.И., Нигматуллина А.Н. Теория информационной безопасности и методология защиты информации: учебное пособие. – Казань: КГТУ, 2008. – С. 358.