**Айрапетян Роберт Артемович. Методи захисту програмного забезпечення від несанкціонованого доступу та шкідливих програм : Дис... канд. наук: 05.13.21 - 2009.**

|  |  |
| --- | --- |
| |  | | --- | | **Айрапетян Р.А. Методи захисту програмного забезпечення від несанкціонованого доступу й шкідливих програм. Рукопис.**  Дисертація на здобуття наукового ступеня кандидата наук за фахом 05.13.21 системи захисту інформації – Одеська національна академія зв’язку ім. О. С. Попова Одеса, 2009.  Метою дослідження є підвищення безпеки програмних продуктів, а саме надійності захисту від несанкціонованого доступу (НСД) шляхом розробки нових моделей та методів протидії дослідженню коду, а також збільшення кількості знайдених шкідливих програм шляхом безпечного їх розпакування.  Побудовано моделі захисту ПЗ на основі важкооборотних задач і методи на їх основі, що використовують завдання про Гамільтонов цикл на графі й задачу на мережах Петрі. На цьому створені інструментальні засоби, що дозволяють захистити здійсненний модуль програми від дослідження й злому на настільних й кишенькових персональних комп'ютерах.  Розроблено підхід для програмно-апаратного захисту, заснований на спеціальному пристрої, що виконує окремі процедури програми, що захищається, і в такий спосіб дозволяє захистити й прискорити виконання коду.  Розроблено новий метод для універсальної розпаковки шкідливих програм в безпечному оточенні, а також програмний комплекс для вивчення й захисту від шкідливого ПЗ. Запропонований метод використаний у розробці антивірусного ПЗ. | |
| |  | | --- | | У дисертації вирішені науково-практичні задачі розроблені нові методи захисту ПЗ від несанкціонованого доступу та шкідливих програм. Основні результати дисертаційної роботи наступні:  1. Проведено аналіз існуючих рішень в області захисту інформації й, зокрема, програм. Зроблено висновок, що існуючі методи захисту ПЗ мають потребу в удосконаленнях для ускладнення пошуку ключа, а також налагодження й дизасемблювання. Виявлено необхідність розробки універсального методу розпакування програм у зв'язку з тим, що більшість шкідливих програм запаковані для ускладнення аналізу антивірусами.  2. Розроблено узагальнені моделі для симетричної і комбінованої систем захисту програм, що дозволяють здійснити захист ПЗ на 2-х рівнях: від знаходження секретного ключа і від вивчення.  3. Розроблено програмні методи захисту ПЗ на основі важкооборотних задач (знаходження Гамільтонова циклу на графі; визначення початкової розмітки мережі Петрі). Знаходження досить великого ключа (більше 64 біт) є трудомісткою NP-повною обчислювальною задачею.  4. Створено інструментальні засоби, що дозволяють захистити програми, що виконуються, розробленими методами на настільному й кишеньковому персональному комп'ютерах, причому, для кишенькових комп'ютерів подібний засіб створений вперше. Захист впроваджений у продукцію таких компаній як Landpro Systems, DL Software, RDM Distributing, Inc., ARlab, corecodec inc. і інших.  5. Запропоновано програмно-апаратний механізм захисту, заснований на спеціальному захисному пристрої, що виконує окремі процедури програми. Встановлено, що злом такого захисту є трудомістким завданням, тому що при розмірі вхідних параметрів захищеної функції *n* = 32, розмірі вихідних параметрів *m* = 32 і часу подачі вхідних параметрів до одержання вихідних *t* = 1 мс для побудови таблиці відповідностей необхідно затратити 49,7 доби.  6. Розроблено новий метод для вивчення шкідливого ПЗ, заснований на універсальному розпакуванні програми в пам'яті, що дозволяє збільшити кількість знайдених шкідливих програм на 18% у порівнянні зі стандартним сигнатурним пошуком, та впроваджено в антивірусний засіб. Також створена система CAMDPAMS для автоматизації процесів збору, вивчення й аналізу шкідливих програм і управління антивірусними лабораторіями компанії Comodo group.  7. Розроблені моделі й методи впроваджені в навчальний процес кафедри системного програмного забезпечення ОНПУ в дисциплінах «Надійність та захист програмного забезпечення», «Системне програмування і операційні системи» і в дипломних проектах. | |