***Практическая работа № 16***

**Использование методов и средств защиты программного обеспечения**

*Цель работы:* изучение опыта использования методов и средств защиты ПО

*Теоретическое обоснование*

В общем случае технологическая схема защиты может состоять из следующих этапов:

|  |  |
| --- | --- |
| —  входной контроль новых программ;  —  сегментация информации на магнитном диске; | —  защита операционной системы от заражения;  —  систематический контроль целостности информации. |

В состав программного комплекса должны входить следующие компоненты.

|  |  |
| --- | --- |
| —         *Каталог детекторов.*  —         *Программа для вакцинации.*  —       *Резидентные средства защиты.* | —         *Программа-ловушка вирусов.*  —       *База данных о вирусах и их характеристиках.* |

1. Методы защиты программ от исследования

Защищаемая от исследования программа должна включать следующие компоненты:

* инициализатор;
* зашифрованную секретную часть;
* деструктор (деициниализатор).

Для большей надежности инициализатор может быть частично зашифрован и по мере выполнения может дешифровать сам себя. Дешифроваться по мере выполнения может и секретная часть программы. Такое дешифрование называется динамическим дешифрованием исполняемого кода. В этом случае очередные участки программ перед непосредственным исполнением расшифровываются, а после исполнения сразу уничтожаются.

Для защиты программ от исследования с помощью дизассемблеров можно использовать и такой способ, как усложнение структуры самой программы с целью запутывания злоумышленника, который дизассемблирует эту программу. Например, можно использовать разные сегменты адреса для обращения к одной и той же области памяти. В этом случае злоумышленнику будет трудно догадаться, что на самом деле программа работает с одной и той же областью памяти.

2.Методы защиты программ от несанкционированных изменений

Наиболее эффективными методами защиты от злоумышленных действий предоставляют криптографические методы защиты.

Для установления подлинности (неизменности) программ необходимо использовать более сложные методы, такие как аутентификация кода программ, с использованием криптографических способов, которые обнаруживают следы, остающиеся после внесения преднамеренных искажений.

Можно еще более усложнить действия злоумышленника по нарушению целостности целевых программ, используя схемы подписи с верификацией по запросу

* Основные методы защиты от копирования
* *Криптографические методы*
* с использованием односторонней функции;
* с использованием шифрования.
* *Метод привязки к идентификатору*
* *Методы, основанные на работа с переходами и стеком*
* *Манипуляции с кодом программы*
* включение в тело программы «пустых» модулей;
* изменение защищаемой программы.

3. Методы противодействия динамическим способам снятия защиты программ от копирования

* *Периодический подсчет контрольной суммы, занимаемой образом задачи области оперативной памяти, в процессе выполнения. Это позволяет:*
  + заметить изменения, внесенные в загрузочный модуль;
  + в случае, если программу пытаются «раздеть», выявить контрольные точки, установленные отладчиком.
* Проверка *количества свободной памяти и сравнение и с тем объемом, к которому задача «привыкла» или «приучена».*
* *Проверка содержимого незадействованных для решения защищаемой программы областей памяти, которые не попадают под общее распределение оперативной памяти, доступной для программиста, что позволяет добиться «монопольного» режима работы программы.*
* *Проверка содержимого векторов прерываний (особенно 13h и 21h) на наличие тех значений, к которым задача «приучена».*
* *Переустановка векторов прерываний.*
* *Постоянное чередование команд разрешения и запрещения прерывания, что затрудняет установку отладчиком контрольных точек.*
* *Контроль времени выполнения отдельных частей программы, что позволяет выявить «остановы» в теле исполняемого модуля.*

*Методические указания*

Для выполнения практической работы воспользуйтесь ссылкой:

* Безопасность программного обеспечения компьютерных систем — <http://citforum.ru/security/articles/kazarin/3.shtml>
* АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ: УЧЕБНОЕ ПОСОБИЕ. Автор/создатель: Варлатая С.К., Шаханова М.В. — <http://window.edu.ru/catalog/pdf2txt/903/49903/24552?p_page=1>

*Задания*

1. Повторите теоретический материал
2. Составьте список основных *методов* защиты ПО
3. Составьте список основных *средств* защиты ПО
4. При помощи интернета исследуйте опыт использования методов и средств защиты ПО на различных сайтах и форумах
5. Запишите анализ полученной информации и выводы в тетрадь
6. Проведите собственное исследование – установите антивирусные средства на свой ПК по очереди, протестируйте их и опишите полученные результаты. (этот пункт выполнять необязательно)

*Контрольные вопросы*

1. Назовите методы защиты программ от исследования
2. Назовите методы защиты программ от несанкционированных изменений
3. Назовите методы защиты программ от копирования
4. Назовите методы защиты противодействия динамическим способам снятия защиты программ от копирования
5. Назовите наиболее действенные средства защиты ПО

*Форма отчёта*

Конспект, проверка письменной работы, ответы на вопросы