МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Новоуральский технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(НТИ НИЯУ МИФИ)
Колледж НТИ

Цикловая методическая комиссия информационных технологий

ОТЧЕТ №3
ПО ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЕ НА ТЕМУ

«Механизмы контроля целостности данных»

ОП.01 «Защита информации в КС»

Специальность СПО 09.02.03
«Программирование в компьютерных системах»

очная форма обучения
на базе основного общего образования

Выполнил
студент группы КПР–47 Д
Егорушкин И.А. _____14.10.2020_____ _____
дата подпись

Проверил
преподаватель _____ _____
Горницкая И.И. дата подпись

Новоуральск 2020

Цель: ознакомление с базовыми технологиями взлома программных защит

КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ОТЧЁТА

1. Какие существуют способы обхода защиты с помощью ключевого диска?

Обойти защиту с помощью ключевого диска можно несколькими способами. Самый простой способ - копирование ключевого диска. Напомним, что большинство традиционных методов рассчитано на невозможность для стандартной программы-копировщика создания копии ключевого диска.

2. В чём заключается технология взлома защит, основанных на ключевом сравнении?

Для взлома нарушителю прежде всего необходимо изучить код защищенной программы и понять логику работы защитного механизма.

Поэтому первый шаг взломщика - дизассемблирование программы.

Второй шаг взломщика - поиск команды сравнения ключа и веток условного перехода.

Тратим шагом внести корректирующие изменения.

3. В чём проявляется уязвимость криптографических систем защиты?

Поблочное дешифрование. Расшифровывание кода программы следует производить поэтапно, часть за частью, добиваясь того, чтобы полностью в открытом виде исполняемый код никогда бы не находился в памяти.

Шифрование с обратной связью. Необходимо реализовать схему, в которой ключ для дешифрования фрагментов кода изменяется динамически и зависит от ранее полученных значений или условий, например, вычисляется как функция от предыдущего блока (возможны варианты).

Использовать контрольную сумму исполняемого кода для расшифровки фрагмента кода.

Специалисты предлагают часть механизма защиты оформить в виде резидентного модуля, в задачу которого могут входить, например, запрещение записи на диск в течение некоторого времени или контроль сегментных регистров на предмет изменения. При этом желательно организовать защиту так, чтобы коды защитного механизма всегда попадали в дамп вместе с кодами основной программы.

Комбинирование криптографических методов со сжатием. В этом случае копию расшифрованного участка нельзя будет вписать на то же место.

4. В чём заключается сущность атаки полным перебором?

Суть заключается в полном переборе значений.

Вывод: входе практической работы били изучены с базовые технологиями взлома программных защит