

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УДК 004.056.2

Политехнический институт  
Факультет приборостроения,  
информационных технологий и  
электроники

Выпускающая кафедра:  
Информационная безопасность систем  
и технологий  
Учебная группа 12ПИ1

УТВЕРЖДАЮ

Зав. кафедрой ИБСТ

к.т.н., доцент

С.Л. Зефиров

«\_\_» \_\_\_\_\_ 2017 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ  
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ  
РАБОТУ**

студента группы 12ПИ1 Клементьева Михаила Андреевича

Специальность 100503 – Информационная безопасность  
автоматизированных систем

Тема дипломного проекта: Выявление вредоносного программного  
обеспечения, внедренного в ядро Linux.

Руководитель ВКР

Старший аналитик информационной безопасности ООО «Диджитал  
Секьюрити» Бажин Роман Валерьевич

Нормоконтролер

к.т.н., доцент

Иванов А.П.

## **1 Цели и задачи ВКР**

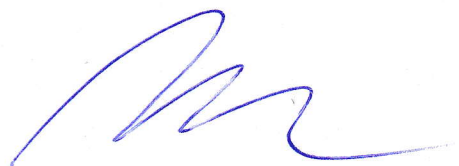
Цель работы: разработка методов выявления вредоносного программного обеспечения, внедренного в ядро Linux.

ВКР направлена на разработку новых методов обнаружения компрометации системы вредоносным программным обеспечением на уровне ядра Linux. Разрабатываемые методы предназначены для выявления скрытых вредоносным ПО процессов, объектов файловой системы и сетевых соединений.

## **2 Тактико-технические требования к выполнению ВКР**

Технические требования к методам выявления вредоносного программного обеспечения:

- методы должны обеспечивать выявления вредоносного программного обеспечения, производящего скрытие процессов операционной системы;
- методы должны обеспечивать выявления вредоносного программного обеспечения, производящего скрытие сетевых соединений;
- методы должны обеспечивать выявления вредоносного программного обеспечения, производящего скрытие объектов файловой системы;
- методы должны обеспечивать защиту от противодействия своей работе со стороны вредоносного программного обеспечения на уровне ядра операционной системы;
- для выполнения ВКР необходимо следующее программно-аппаратное обеспечение:
  - компьютер с установленной операционной системой GNU/Linux;
  - GNU C Compiler.



В ВКР должны быть рассмотрены следующие вопросы:

- описание существующих методов обнаружения руткитов, внедренных в ядро Linux;
- описание разработанных методов;
- разработка алгоритмов выявления вредоносного программного обеспечения;
- разработка и описание средства по обнаружению компрометации ядра;
- разработка и описание методики настройки и эксплуатации средства обнаружения компрометации ядра;
- результаты экспериментальных исследований разработанных алгоритмов.

### **3 Требования к разрабатываемой документации**

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- алгоритм функционирования метода выявления скрытых процессов – 1 л., ф. А1 (плакат);
- алгоритм функционирования метода выявления скрытых сетевых соединений – 1 л., ф. А1 (плакат);
- алгоритм функционирования метода выявления скрытых объектов файловой системы – 1 л., ф. А1 (плакат);
- схема планировщика задач ядра Linux;
- схема слоя виртуальных файловых систем ядра Linux;
- схема сетевого стека ядра Linux;
- демонстрация выполнения разработанных методов.





Электронная копия отчета и графической части ВКР должна быть представлена на оптическом носителе.

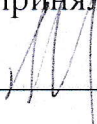
#### **4 Сроки выполнения ВКР**

Тема утверждена приказом ректора ПГУ № 472 от «26» апреля 2017 г.

Дата выдачи задания «16» февраля 2017 г.

Время дипломного проектирования с 13.02.2017 г. по 04.06.2017 г.

Задание к исполнению принял «16» февраля 2017 г.

Исполнитель ВКР  Клементьев М. А.

