Digital Security
БЕЗОПАСНОСТЬ КАК ИСКУССТВО

197046, Санкт-Петербург
Петроградская набережная, дом 16 литера А
+7 (812) 703-15-47
www.dsec.ru, info@dsec.ru

ОТЗЫВ

на дипломный проект студента ФГБОУ ВО «Пензенский государственный университет»

специальности 10.05.03 «Информационная безопасность автоматизированных систем»

Клементьева Михаила Андреевича

на тему: «Выявление вредоносного программного обеспечения, внедренного в ядро Linux»

Дипломный проект Клементьева М. А. посвящен анализу существующих и выработке новых методов для борьбы с вредоносным программным обеспечением. Актуальность выбранной им темы определяется тем, что на данный момент существует недостаток в эффективных методах и средствах обнаружения руткитов на рабочих станциях и серверах под управлением операционных систем GNU/Linux.

Пояснительная записка построена логично и последовательно отражает все этапы проведенного исследования. Подробно рассмотрены подсистемы ядра Linux, ключевые механизмы работы ядерных руткитов и техники, которые используются вредоносным программным обеспечением при скрытии различных процессов в операционной системе.

Описаны существующие методы и средства выявления руткитов на примере доступного свободного программного обеспечения, используемого системными администраторами в работе.

Во время выполнения дипломного проекта были разработаны и подробно описаны методы по выявлению вредоносного программного обеспечения на уровне ядра, каждый метод был реализован и протестирован.

Экспериментальное исследование разработанных алгоритмов показало их эффективность в противодействии исследовательским образцам вредоносного программного обеспечения, тем самым показав их применимость к решению реальных задач.

Дипломный проект выполнен технически грамотно, в полном соответствии с техническим заданием на проектирование и заслуживает оценки отлично.

Научный руководитель: _____ Бажин Р. В.