ОТЗЫВ

научного руководителя на диссертационную работу

Гибилинды Романа Владимировича

«Разработка автоматизированных методов анализа воздействий на файлы в задаче расследования инцидентов информационной безопасности»,

представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Гибилинда Роман Владимирович в 2014 году с отличием окончил Институт радиоэлектроники и информационных технологий-РтФ УрФУ по специальности 090106 «Информационная безопасность телекоммуникационных систем». На старших курсах проявил интерес к научно-исследовательской работе.

С марта 2014 г. по август 2015 г. Гибилинда Р.В. работал в ООО «Горизонт», где занимал должность инженера-проектировщика; с сентября 2015 по настоящее время является военнослужащим. С октября 2018 г. по настоящее время Роман Владимирович по совместительству работает в должности ассистента Института радиоэлектроники и информационных технологий-РтФ. За время работы Р.В. Гибилинда показал себя целеустремлённым исследователем, способным самостоятельно ставить и решать сложные научно-технические задачи, имеющие научное и практическое значение, овладевать современными теоретическими методами анализа и интерпретировать результаты исследований. Роман Владимирович проявил высокую организованность, работоспособность и трудолюбие.

За время своей работы Гибилинда Р.В. выполнил ряд научно-исследовательских работ, по результатам которых опубликовано 6 научных работ, из них 4 статьи опубликованы в рецензируемых научных журналах и изданиях, определенных ВАК и Аттестационным советом УрФУ, включая 1 статью в издании, индексируемом в международной цитатно-аналитической базе Scopus. Имеются 2 свидетельства о государственной регистрации программы для ЭВМ.

Диссертационная работа Гибилинды Р.В. соответствует паспорту специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность. Научная новизна диссертационного исследования Р.В. Гибилинды заключается в разработке событийной модели процесса идентификации воздействий на файлы, основанной на математическом аппарате сетей Петри, впервые учитывающей признаки, характеризующие файл, и совершенные над ним файловые операции; создании кластеризационного метода идентификации воздействий на файлы, впервые использующего адаптированные алгоритмы предварительной подготовки входных данных и определения оптимального количества

кластеров. Предложен метод экспресс-анализа событий информационной безопасности, связанных с воздействиями на файлы, позволяющий выявлять аномальные, условно аномальные и нормальные воздействия на файлы в ходе расследования инцидента информационной безопасности (ИБ).

Теоретическая значимость работы заключается в совершенствовании методов анализа массивов данных в целях автоматизации процесса расследования инцидентов ИБ.

Практическая значимость работы состоит в разработке комплекса программных средств, позволяющего в ходе расследования инцидента ИБ автоматизировать процесс анализа журнала изменений тома $UsnJrnl для идентификации, обнаружения и классификации воздействий на файлы с целью определения событий и хода инцидента ИБ.

Диссертационная работа Гибилинды Р.В. выполнена на высоком уровне и соответствует существующим требованиям. Результаты работ в полной мере представлены в публикациях на тему диссертации.

Считаю, что Гибилинда Роман Владимирович достоин присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Научный руководитель, доцент учебно-научного
центра «Информационная безопасность»
Института радиоэлектроники и
информационных технологий-РтФ,
ФГАОУ ВО «УрФУ имени первого
Президента России Б.Н. Ельцина»
кандидат технических наук, доцент,
620002, Россия, г. Екатеринбург, ул. Мира 19,
Тел.: +7 (343) 3759557
E-mail: n.i.sinadsky@urfu.ru

_____Николай Игоревич Синадский

24.02.2021

Подпись Синадского Н.И. заверяю
Ученый секретарь
Ученого совета УрФУ

_____ В.А. Морозова

25 02 2021 г.