ЦЕНТР ПОДДЕРЖКИ ТЕХНОЛОГИЙ И ИННОВАЦИЙ

ДАЙДЖЕСТ

«ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ УЧЁНЫХ-ИЗОБРЕТАТЕЛЕЙ РОССИЙСКИХ РЕГИОНОВ. ТВЕРСКАЯ ОБЛАСТЬ»

Приурочен к ГОДУ НАУКИ И ТЕХНОЛОГИЙ

В рамках просветительского проекта Центров поддержки технологий и инноваций

2021

Дроботун Евгений Борисович

профессор кафедры «Тактики и вооружения радиотехнических войск» Военной академии воздушно-космической обороны имени Маршала Советского Союза Г. К. Жукова, доктор технических наук

Родился 20 октября 1974 года в городе Павлодар Казахской ССР.

Образование:

1) Санкт-Петербургское высшее училище радиоэлектроники противовоздушной обороны – 1997 г.
2) Военная академия воздушно-космической обороны имени Маршала Советского Союза Г. К. Жукова (адъюнктура) – 2009 г.
3) Военная академия воздушно-космической обороны имени Маршала Советского Союза Г. К. Жукова (докторантура) – 2018 г.

Кандидат технических наук – 2009 г.

Доктор технических наук – 2019 г.

Сфера деятельности:

Подготовка офицеров для Воздушно-космических сил Российской Федерации. Проведение научных исследований и работ, связанных с совершенствованием как объектов учебно-материальной базы академии, так и образцов вооружения и военной техники противовоздушной обороны.

Автор 96 опубликованных научных работ, в том числе 2 монографий, 10 патентов РФ, 3 из которых включены в БД Перспективные российские изобретения ФИПС РОСПАТЕНТ.

Патент РФ № 2630163

СПОСОБ КОНТРОЛЯ ДОСТУПА К ФАЙЛАМ

Изобретение относится к вычислительной технике, а именно к защите от несанкционированного доступа к информации, обрабатываемой и хранимой в информационно-вычислительных системах различного назначения. Технический результат – снижение времени обращения к файлам при контроле прав доступа к ним и соответственно повышение быстродействия информационно-вычислительной системы в целом. Способ контроля доступа к файлам заключается в предварительном (на этапе получения доступа к операционной системе пользователем, после его идентификации) формировании списков файлов, с которыми пользователю разрешено проводить различные действия. При этом для каждого действия формируются свои списки, которые после входа пользователя помещаются в оперативную память, в область, недоступную для несанкционированного доступа.

Патент РФ № 262374

СПОСОБ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Изобретение относится к области систем защиты автоматизированных систем управления различного назначения от информационно-технических воздействий и может быть использовано для построения систем защиты автоматизированных систем управления (АСУ) от одного из основных видов информационно-технических воздействий - компьютерных атак. Технический результат, заключающийся в получении наиболее эффективного варианта построения системы защиты АСУ от компьютерных атак с наименьшим

воздействием на производительность защищаемой АСУ, достигается за счет использования способа построения системы защиты АСУ от компьютерных атак, включающего в себя этап формирования множества всех возможных вариантов построения подсистем системы защиты АСУ от компьютерных атак, этап формирования множества всех возможных вариантов построения системы защиты АСУ от компьютерных атак, этап оценки стоимости и требуемых ресурсов вариантов построения системы защиты АСУ от компьютерных атак, этап оценки эффективности вариантов построения системы защиты АСУ от компьютерных атак и этап оценки степени влияния вариантов построения системы защиты на производительность защищаемой АСУ.

Патент РФ № 2640629

СПОСОБ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Изобретение относится к способу оценки эффективности функционирования автоматизированных систем управления (АСУ). Технический результат заключается в расширении функциональных возможностей способа оценки эффективности АСУ за счет добавления в него процесса моделирования воздействия вредоносных программ на структурные элементы АСУ. Способ включает в себя выбор стратегии оценки эффективности управления; моделирование воздействие вредоносных программ на структурные элементы (СЭ) АСУ, которые осуществляют прием, хранение, обработку, выдачу и отображение информации, путем внедрения образцов вредоносного кода в память этих СЭ АСУ с помощью устройства моделирования воздействия вредоносных программ, на основе информации об уязвимостях программного и аппаратного обеспечения СЭ АСУ, полученной из запоминающего устройства (ЗУ) уязвимостей, ЗУ весовых коэффициентов, соответствующих критичности каждой уязвимости и ЗУ образцов вредоносного кода; затем автоматически считывают информацию с датчиков через преобразователи и записывают ее в ЗУ считанной информации терминального сервера, в котором преобразуют эту информацию к виду, удобному для текущей оценки, а затем оценивают ее по программе оценки эффективности управления.