

В данной работе рассматриваются информационные объекты информационного пространства на более высоком уровне абстракции и понятии управления информационным объектом.

Информационный объект управляемый, если существует и может быть применен алгоритм управления этим объектом. Существует три типа управляемости информационного объекта: тотальная, частичная и скрытная.

Управление информационным объектом опирается на контроль за ним: полный и частичный.

В зависимости от роли моделей информационного объекта в информационном пространстве (социальные сети, Интернет) их можно классифицировать на: невидимые, тривиальные и опасные.

Изложенные основы позволяют сформулировать основные аксиомы, решением задач с использованием математического моделирования в рамках которых и занимается формальная теория информационных войн.

Литература

1. *Рассторгуев С.П.* Информационная война. Проблемы и модели. М., 2006.
2. *Рассторгуев С.П.* Математические модели в информационном противоборстве. Экзистенциальная математика. М., 2014.
3. «Глобальные тенденции 2030: Альтернативные миры» (Global Trends 2030: Alternative Worlds) — пятый выпуск докладов Национального Совета по разведке — www.nkibrics.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

В.М. Алефиренко

Антивирусные программные средства широко используются для защиты компьютерной техники от различного рода вирусов. Как правило, пользователь выбирает то или иное антивирусное средство, основываясь на общих представлениях о его возможностях. В то же время каждое антивирусное средство характеризуется целым рядом параметров, значения которых в совокупности определяют его уровень качества. Поэтому выбор наиболее оптимального по своим параметрам антивирусного средства представляет определенный интерес для пользователей компьютерной техники. Для сравнительного анализа антивирусных средств предлагается использовать комплексный метод определения уровня качества с использованием соответствующих единичных показателей. В качестве единичных показателей для средств антивирусной защиты были выбраны их основные параметры, такие как коэффициент надежности защиты, время сканирования файлов, время копирования файлов, замедление старта офисных программ, а также цена (стоимость на момент исследования). Для сравнения были выбраны следующие антивирусные средства: Avast Professional, AVG Anti-Virus & Anti-Spyware, Avira AntiVir PE Premium, Dr.Web Anti-Virus, Eset NOD32 Antivirus, Norton AntiVirus и Kaspersky Anti-Virus. Расчет проводился с использованием средневзвешенного арифметического показателя, характеризующего комплексный показатель качества. Предварительно было проведено нормирование единичных показателей (значений параметров) и соответствующих им коэффициентов значимости. В результате расчетов были получены следующие значения комплексного показателя качества (в порядке убывания): Avira AntiVir PE Premium — 0,863; Avast Professional — 0,712; Kaspersky Anti-Virus — 0,655; Norton AntiVirus — 0,585; Eset NOD32 Antivirus — 0,518; Dr.Web Anti-Virus — 0,415.

Таким образом, использование комплексного показателя качества позволило провести сравнительный анализ программных средств антивирусной защиты. Однако следует отметить, что эти результаты носят оценочный характер и не могут являться абсолютным критерием для выбора того или иного антивирусного средства для защиты компьютерной техники от различного рода вирусов.

ПРОГРАММНЫЙ КОМПЛЕКС МОДЕЛИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ АТМ ТЕРМИНАЛОВ

Алзамили Али Хасан Вахид, Т.В. Борботько

Современные автоматизированные банковские системы предоставляют возможность проведения удаленных банковских транзакций, что, несомненно, является их преимуществом для клиентов по сравнению с расчетно-кассовым их обслуживанием. Однако необходимо отметить, что удаленные банковские терминалы, такие как автоматические кассовые аппараты (АТМ – automatic