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. *Расторгуев С.П.* Информационная война. Проблемы и модели. М., 2006.

2. *Расторгуев 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 рассчетно-кассовым их обслуживанием. Однако необходимо отметить, что удаленные банковские терминалы, такие как автоматические кассовые аппараты (ATM – automatic

teller machine), являются наиболее уязвимым элементом системы дистанционного банковского обслуживания.

В настоящее время номенклатура средств обеспечения безопасности банковских терминалов достаточно широкая и при проектировании таких систем, специалист должен уметь обоснованно выбирать технические средства защиты, позволяющие противодействовать соответствующим угрозам безопасности для такого типа оборудования. Таким образом, обучение специалистов по защите информации и повышение их квалификации является актуальной проблемой, для решения которой, в части обеспечения безопасности АТМ терминалов, разработан программный комплекс (ПК).

В качестве среды разработки указанного комплекса использовался программный пакет Macromedia Flash, отличительной особенностью которого является наличие собственного языка программирования ActionScript. Проектирование системы безопасности АТМ, с использованием разработанного ПК выполняется с учетом места установки банковского терминала, исходя из чего пользователь из предлагаемого перечня угроз выбирает наиболее вероятные. На втором этапе выбираются средства обеспечения безопасности, которые, по мнению пользователя, позволяют противодействовать угрозам, определенным на предыдущем этапе. Выбор средств усложняется тем, что учитывается лимит денежных средств, доступных для приобретения таких средств защиты. Пользователь не может завершить проектирование системы безопасности, в случае если лимит денежных средств исчерпан. По завершению проектирования, ПК проводит анализ правильности действий пользователя в части перечня угроз, которые он определит и выбранных средств защиты. По завершению анализа программа формирует отчет, в котором отмечаются ошибки совершенные пользователем на этапе проектирования, для исправления которых необходимо вновь выполнить вышеуказанные этапы 1 и 2.

Разработанный ПК позволяет получить практические навыки при проектировании системы безопасности АТМ терминалов с учетом различных вариантов их установки, а так же выделяемого лимита денежных средств на приобретение средств обеспечения безопасности АТМ.

ВИЗУАЛЬНОЕ ШИФРОВАНИЕ СЕГМЕНТИРОВАННЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПЕРЕСТАНОВОК БИТОВЫХ ПЛОСКОСТЕЙ

Х.М. Альзаки, В.Ю. Цветков, М.Б.М. Махммуд, С.Х. Карбалаи, Ф.Р. Алиханов

Сегментация находит широкое применение в задачах обработки изображений. Сегментированное изображение представляет собой матрицу, совпадающую с размером исходного изображения, каждый элемент которой имеет номер сегмента, которому он принадлежит. Возможно представление сегментированного изображения в виде набора битовых плоскостей, содержащих соответствующие разряды элементов [1]. Предлагается алгоритм визуального шифрования сегментированных изображений на основе перестановок битовых плоскостей. Алгоритм применяет операции поворота на 90 град, зеркальные повороты и диадные сдвиги к каждой битовой плоскости согласно секретным ключевым параметрам. В результате данных операций искажаются значения элементов матрицы сегментации, что приводит к эффекту визуального шифрования, затрудняющего или делающего невозможным восприятие видеоинформации, содержащейся в исходном изображении. Предложенный алгоритм является обратимым и симметричным. Для повышения его стойкости предлагается применять независимо формируемые ключевые последовательности к каждой битовой плоскости.

Литература

1. *Конопелько В.К.* Текстурная сегментация изображений на основе классификации контурных элементов / В.К. Конопелько, С.Н. Касанин, В.Ю. Цветков, Х.М. Альзаки // Вестник сувязі. 2016. № 1. С. 48–52.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

К.М. Бердимырадов

Среди основных требований к проведению коммерческих операций — конфиденциальность, целостность, аутентификация, авторизация, гарантии и сохранение тайны. Для противодействия этим угрозам используется целый ряд методов, основанных на различных технологиях, а именно: шифрование — кодирование данных, препятствующее их прочтению или искажению; цифровые