## ТЕХНОЛОГИЯ СОЗДАНИЯ МАТЕРИАЛОВ НА ОСНОВЕ НАТУРАЛЬНЫХ ПРИРОДНЫХ КОМПОНЕНТОВ

Е.С. БЕЛОУСОВА, А. ОМЕР ДЖАМАЛЬ САД, Ю.В.БЕЛЯЕВ

Использование природных компонентов фона в составе маскировочных материалов значительно снижает контраст с фонами, особенно в полосах поглощения, характерных для определенного класса фонов. При этом необходимо решить задачу сохранения спектральных отражающих свойств защитных материалов в течение длительного времени эксплуатации маскировочных средств, надежную фиксацию природных материалов на используемой подложке и хорошие механические свойства создаваемых конструкций и материалов. Особую актуальность приобретает создание защитных материалов (ЗМ), имитирующих растительность в летнее время. Использование свежесрезанных образцов доминирующей на местности растительности сталкивается с трудностями при долговременном скрытии объекта. Полосы поглощения хлорофилла, определяющие в видимой области спектральные характеристики отраженного излучения, быстро разрушаются, образцы теряют воду, что также сказывается на изменении спектральных свойств отраженного от таких образцов излучения. Авторами предлагается несколько способов создания ЗМ на основе растительной массы на клеевой основе или с покрытием из изолирующих слоев силиконовой пленки.

В качестве одного из вариантов в конструкции ЗМ использовались свежесрезанные листья растительности, уложенные на материал подложки с подготовленной влагоотталкивающей (покрытой силиконом) поверхностью, и сверху также покрытые тонким слоем силикона. Такая укладка листовой ткани между слоев силикона позволяет сохранять влагу в листве и предохраняет хлорофилл от разрушения. При этом спектральные свойства такого материала практически не меняются в течение, как минимум, трех месяцев. Другим вариантом использования растительной массы в конструкциях ЗМ является изготовление смеси высушенного лаврового листа и силикона. Механические прочностные характеристики (стойкость к изгибу) возрастали по мере увеличения доли силикона в смеси, однако контраст коэффициента спектральной яркости таких образцов с образцами живой растительности по мере увеличения доли силикона также возрастал, уменьшая при этом маскировочные свойства.

## ИЗМЕРЕНИЕ КООРДИНАТ В РАДИОЛОКАЦИОННЫХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ МАИ

БЕРДЯЕВ В.С., ЗЕНЬКО П.Н.

Для создания замкнутой автоматизированной системы управления (АСУ) воздушным движением радиолокационную станцию (РЛС) необходимо дополнять устройствами, которые осуществляют слежение за воздушными объектами с высокой точностью и без временной задержки. Преимущества рассматриваемой автоматизированной системы состоят, во-первых, в использовании мелких азимутальных импульсов (МАИ) для измерения координат, что обеспечивает значительное сокращение времени обзора пространства за счет повышения скорости вращения антенны и, во-вторых, в получении синусно-косинусных зависимостей для формирования круговой развертки на основе мелких азимутальных импульсов. Преобразователи дальности и угловых координат в устройстве строятся по одному и тому же принципу счета эталонных импульсов, интервал между которыми соответствует определенной дальности и углу поворота антенны в азимутальной плоскости. Так как требуемое число импульсов азимута отличается от количества импульсов МАИ из-за необходимости строгого соответствия с дальностью развертки на $2\pi$, то имеет место увеличение точности по азимуту. Количество

Библиотека БГУИР

импульсов по двум координатам преобразуется затем в двоичный код и передается в процессор.

Решение проблемы обнаружения воздушных объектов связано прежде всего с защитой сигнала от помех. Полученные с помощью предлагаемого устройства координаты объектов по дальности и азимуту вводятся в символ каждого объекта только после того, как выполнена первичная обработка радиолокационной информации. Она представляет собой защиту от наиболее распространенных помех: хаотических импульсных, детерминированных и непрерывных шумовых.

## ОБ ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КРЕДИТНО-ФИНАНСОВЫХ УЧРЕЖДЕНИЙ НА БАЗЕ ТЕОРИИ ИГР

Е. В. ВАЛАХАНОВИЧ, Л. В. МИХАЙЛОВСКАЯ

В настоящее время термин «информация» все чаще используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость вычислительной системы, в рамках которой он обрабатывается. Жизненно важные интересы всех банковских систем заключаются в том, чтобы информация, касающаяся их деятельности, была бы надежно защищена от неправомерного использования. Одной из важнейших задач защиты информационных ресурсов в банковских системах является минимизация рисков. Под риском понимаются возможные потери вследствие воздействия угроз через уязвимые места системы.

Использование натурного эксперимента для оценки рисков и их минимизации трудно осуществимо из-за колоссальных материальных затрат, высокой трудоемкости и невозможности охвата всех сочетаний воздействующих угроз и режимов функционирования банковских систем.

В связи с этим математическое моделирование оценки рисков от возможных угроз представляется наиболее перспективным с точки зрения обеспечения заданной точности, адекватности моделей и результатов расчета, а также материальных затрат и времени проведения расчетов. Математическое моделирование оценки рисков позволяет решать задачи, включающие элементы непрерывного и дискретного действия с учетом факторов случайного воздействия.

Из математических методов оценки рисков наиболее предпочтительными представляются методы, основанные на базе теории игр. В случае необходимости минимизировать суммарные риски целесообразно применять алгоритм симплекс-метода. Если же ставится задача определить наилучшую среди стратегий, то для оценки рисков банковских систем удобно использовать антагонистические игры в нормальной форме, реализуя принцип минимакса. Если в ходе моделирования кроме личных ходов необходимо учесть и случайные ходы, то выигрыш при паре стратегий есть величина случайная, зависящая от исходов всех случайных ходов. В этом случае естественной оценкой возможного выигрыша является математическое ожидание случайного выигрыша.

Таким образом, методы теории игр позволяют при минимальных затратах сформировать адекватную стратегию по информационной безопасности для кредитно-финансовых учреждений.

Библиотека БГУИР