Целью исследования состоит в определении и реконструкции основных принципов процесса принятия экономического решения на базе анализа фактора неопределенности.

Принятие решений в условиях неопределенности характерны тем, что субъекту, принимающему рискованное решение неизвестны вероятности различных вариантов развития событий, связанных с принимаемым решением. В этом случае при выборе альтернативы принимаемого решения субъект руководствуется, с одной стороны, своим рисковым предпочтением, а с другой – соответствующим критерием выбора из всех альтернатив по составленной им матрице решений.

Принятие решений в условиях риска основано на том, что каждой возможной ситуации развития событий может быть задана определенная вероятность его осуществления. Это позволяет установить весовые коэффициенты каждого из конкретных значений эффективности по альтернативам и по значению вероятности. В результате можно получить на этой основе интегральный показатель уровня риска, соответствующий каждой из альтернатив принятия решений. Сравнение этого интегрального показателя по отдельным альтернативам позволяет избрать для реализации ту из них, которая приводит к заданному показателю эффективности с наименьшим уровнем риска.

**Литература**

1. Диев В.С. Рациональный выбор в условиях риска: модели и парадоксы // Вестн. Новосиб. гос. ун-та. Серия: Философия. 2010. Т. 8, вып. 2. С. 24–31.

## ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ ЗАЩИЩЕННОЙ МУЛЬТИСЕРВИСНОЙ СЕТИ

С.Ю. Лоскот, А.В. Мурашко, О.А. Хацкевич

Для эффективной разработки и внедрения в эксплуатацию мультисервисных сетей связи необходимо предусмотреть своевременную защиту программ и баз данных, средств хранения, обработки и передачи информации. Основные требования предъявляемые к мультисервисной сети связи заключаются в следующем: высокий уровень информационной безопасности; организация четкой аутентификации и идентификации всех пользователей автоматизированной информационной системы; организация системы централизованного управления и др. [1].

В качестве объекта исследования в данной работе была выбрана сеть связи крупного государственного предприятия ЗАО «Технопром». Компания имеет два офиса. Каждый офис имеет собственную локальную сеть. Суммарное количество рабочих станций в двух локальных сетях 500. Пользователи имеют доступ к серверу базы данных, где хранится информация о клиентах, электронной почте и HTTP-серверу. Некоторые сотрудники компании загружают мультимедиа контент, замедляя доступ к сети Интернет другим сотрудникам. В целях обеспечения необходимо уровня безопасности и оптимизации работы мультисервисной сети компания решает установить брандмауэр.

Моделирование мультисервисной сети производилось в программе Riverbed Modeler 17.5. Программный продукт Riverbed Modeler 17.5 – это объектно-ориентированный инструмент моделирования сетей связи. Данная программа имеет обширный пакет различных моделей сетевых элементов, библиотеки различных протоколов сетей связи и позволяет производить расчет основных характеристик с учетом параметров QoS для различных типов трафика [2]. Результаты моделирования представлены в виде графиков, которые отражают процент загрузки WAN соединения, время отклика приложения базы данных и время отклика web страницы.

Было смоделировано два случая работы сети: без установки брандмауэра и с установленным брандмауэром. При моделировании в первом случае были получены следующие данные: время отклика приложения базы данных составляет более 1 сек.; время отклика web страницы – более 3 сек.; процент загрузки WAN соединения равен в среднем 80 %, что приводит к некорректной работе приложений в сети. При моделировании во втором случае были получены следующие данные: время отклика приложения базы данных составляет 1 сек.; время отклика web страницы 3 сек.; процент загрузки WAN соединения уменьшился с 80 % до 40 %.

Результаты исследований показывают, что при использовании в сети устройства защиты от несанкционированного доступа и его правильной конфигурации удалось оптимизировать работу мультисервисной сети, улучшить ее производительность и обеспечить необходимый уровень безопасности.

**Литература**

1. Мультисервисные сети следующего поколения [Электронный ресурс]. – URL: http://www.iksmedia.ru/articles/718285-Multiservisnye-seti-sleduyushhego.html (дата обращения: 16.05.2018).

2. Проектирование и моделирование сетей связи в системе Riverbed Modeler / В.Н. Тарасов [и др.]. Самара, 2016. 260 с.

## ПОДХОДЫ К ДЕТЕКЦИИ ОБЪЕКТОВ НА ДИНАМИЧЕСКИХ ИЗОБРАЖЕНИЯХ

М.М. Лукашевич

Видеоанатитика в целом и задача детекции объектов на видео в частности являются важными элементами инженерно-технической защиты объектов. Традиционные подходы к детекции объектов на статических или динамических изображениях (видео) включают в себя следующие этапы: сегментация, извлечение признаков и детекция. На этапе сегментации возможно преобразование цветового пространства и применение различных алгоритмов пороговой обработки. В качестве информативных признаков могу использоваться детекторы границ, HOG-признаки, вейвлеты Хаара, Фурье-дескрипторы и др. Детекция и/или распознавание объектов реализуется на базе таких алгоритмов, как SVM классификатор, kNN классификатор, сравнение с эталоном и др.

Типовые схемы не всегда дают требуемую точность детекции. Последние результаты в области глубоких нейронных сетей позволяют улучшить точность детекции объектов. В настоящее время предложено большое число моделей глубоких нейронных сетей. Предложена схема детекции объектов на основе RCNN-детектора [1], состоящего из CNN (сверточной нейронной сети) и классификатора. В частности, предполагается рассмотрение гипотез о метаположении объекта (~2000 К). Гипотезами считаются вырезанные фрагменты изображения, которые подвергаются перемасштабированию. Далее функционирует CNN и вычисляются признаки, на основе которых на следующем этапе выполняется литейная классификация для каждого класса и уточнение местоположения гипотезы. При этом обучается только линейная классификация. Успешность применения глубоких нейронных сетей подтверждена результатами, полученными на массивной базе аннотированных изображений, предназначенной для отработки и тестирования методов распознавания образов и машинного зрения ImageNet [2].

**Литература**

1. Ross Girshick, Jeff Donahue, Trevor Darrell, Jitendra Malik. Rich feature hierarchies for accurate object detection and semantic segmentation Tech report (v5). 22 Oct. 2016.

2. ImageNet [Электронный ресурс]. – URL: http://image-net.org (дата обращения: 16.05.2018).

## МАЙНИНГ КРИПТОВАЛЮТ: НОВЫЕ ВЫЗОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.М. Лыньков, В.С. Князькова

Распространение технологии блокчейн и рост популярности майнинга привели к появлению новых видов угроз информационной безопасности. Сам майнинг представляет собой деятельность по поддержанию работы распределительной сети путем закрытия и создания блоков в технологии блокчейн на основе использования вычислительных мощностей. На данный момент наибольшее распространение получили виды угроз, связанные со скрытым майнингом, а также краже данных криптовалютных кошельков и обменных сервисов.