2. СТБ ГОСТ Р 50840-2000. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости.

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КОНТРОЛЕМ ДОСТУПА В ОБЕСПЕЧЕНИИ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ

А.В. Железняков

Для технической поддержки действий по обеспечению физической защиты объектов и размещенных на них предметов физической защиты применяются комплексы технических средств физической защиты. Комплекс выполняет задачи по сбору, обработке, анализу и контролю всей информации, получаемой от технических средств физической защиты, формирует и передает сообщения подразделениям охраны и органам управления, обеспечивает информационное взаимодействие между пунктами управления, контролирует состояние и работоспособность инженерно-технических средств физической защиты.

В связи с тем, что наиболее вероятным и опасным элементом воздействия на комплекс технических средств физической защиты является человек, то особую роль в комплексе играет система контроля и управление доступом (СКУД).

Главная задача системы контроля управления доступом – сбор полной информации о проникновении на объект.

Функции же СКУД определяются как:

– защита от проникновения на объект лиц без права доступа – благодаря установке СКУД, за ограждение попадают только сотрудники или люди, получившие пропуск.

– защита других лиц, т. е. обеспечить безопасность людей, которые могут по неосторожности попасть на территорию охранных объектов, производства или строек, где можно получить травму;

– контроль за прохождением персонала на территорию объекта, а также сбор информации о длительности пребывания;

– контроль за перемещением сотрудников – эта функция действует, если зоны внутри территории разграничены.

Повышение эффективности использования СКУД возможно наращиванием устройств, подключением интеллектуальных систем видеонаблюдения и др.

СТОХАСТИЧЕСКИЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

А.П. Жук, К.М. Сагдеев, А.А. Гавришев, А.Ю. Муравьев

Современные технологии беспроводной передачи информации (БПИ) активно внедряются и широко используются как в производственной деятельности большинства компаний, так и для построения компьютерных сетей для частного использования. Не смотря на различное назначение систем БПИ, их объединяет одно очень важное обстоятельство – значительный ущерб от нарушения безопасности передаваемой информации [1]. Существующие методы защиты информации в системах БПИ ориентированы, в том числе, на использование криптографических алгоритмов и совершенствование системы аутентификации пользователей. Дальнейшее усложнение существующих или применение более совершенных алгоритмов аутентификации и шифрования передаваемой информации неизбежно сказывается на быстродействии систем БПИ, что снижает показатели качества их функционирования. В связи с этим в докладе поставлена задача усовершенствования методов защиты информации в рассматриваемых системах [2]. Поставленную задачу предлагается решать на основе стохастического преобразования информации универсальным способом, позволяющим обеспечить эффективную защиту данных в системах БПИ [3]. Преимущество данного подхода заключается в том, что в рамках одного алгоритма обеспечивает решение задачи абсолютной секретности в постановке К. Шеннона.

Список литературы

1. Применение сложных сигналов в системах радиосвязи и управления / С.С. Кукушкин [и др.] // Современные тенденции развития науки и технологий. 2015. № 2-2. С.94–96.
2. Осмоловский С.А. Стохастические методы защиты информации. М.: Радио и связь, 2003. 320 с.
3. Жук А.П., Жук Е.П. Способ повышения помехозащищенности систем связи с ортогональными сигналами // Инфокоммуникационные технологии. 2005. Т. 3, № 4. С. 39–41.

ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЫДЕЛЕННОМ ПОМЕЩЕНИИ ПРЕДПРИЯТИЯ

Е.П. Жук, М.А. Брехов, Р.Р. Партоян, Е.В. Черкашин

В настоящее время остро стоит задача обеспечения защиты речевых переговоров от скрытого протоколирования. Для этих целей на предприятиях создаются специальные выделенные помещения, которые оснащаются активными и пассивными средствами защиты информации. В зависимости от корректности предварительного обследования и поиска уязвимостей, строится система защиты информации выделенного помещения, которая имеет конкретную величину стоимости [1]. В данной работе рассматриваются проблемы организации защиты выделенного помещения от несанкционированного съема речевой информации по акустическому каналу, а так же обнаружения уязвимых мест [2].

Известные подходы к построению системы защиты акустической информации в выделенных помещениях ориентированы на достижение конечного результата, заключающегося в обеспечении требуемого уровня защищенности информации без явного учета приемлемого уровня затрат на построение системы защиты. В докладе рассматривается подход, позволяющий учитывать уровень затрат на построение системы защиты акустической информации в выделенном помещении предприятия [3], с учетом уязвимостей, степени конфиденциальности информации и некоторых особенностей вариантов достижения требуемого результата.

Список литературы

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. 436 с.
2. Зашита информации / А.П. Жук [и др.]. М.: РИОР: ИНФРА-М, 2019. 400 с.
3. Жук А.П., Гавришев А.А., Осипов Д.Л. Оценка защищенности беспроводной сигнализации от несанкционированного доступа на основе матрицы нечетких правил // Математические структуры и моделирование. 2016. № 1 (37). С. 112–120.

ФИЛЬТРАЦИЯ СЕГМЕНТНОЙ ПРОЕКЦИИ СИМВОЛЬНОЙ СТРОКИ НА ЭТАПЕ СЕГМЕНТАЦИИ

Д.В. Заерко, В.А. Липницкий

В современную информационную эпоху хранение и передача цифровых сигналов и изображений осуществляется, как правило, в преобразованном или сжатом виде. Процесс их передачи происходит в неизбежно зашумленной среде. Поэтому не подлежит сомнению факт, что в реальных условиях является постоянной проблема восстановления и распознавания переданных изображений. На путях решения этой проблемы накоплен богатый спектр методов и подходов.

Важное место занимает класс изображений с символьной строкой, также подлежащей распознаванию. Типичным примером здесь является сюжет с идентификацией номерных знаков движущегося транспортного средства. В случае основательной зашумленности