Цыганков С.А.
Научный руководитель – к.т.н., доцент каф. ФПМ Штыков Р. А.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
sergei.tsigankow@yandex.ru

Анализ криптографических методов защиты информации системы видеонаблюдения

Самая главная причина использования систем видеонаблюдения - это стремление повысить уровень безопасности и защищенности людей и объектов частной собственности. Следует сказать, что камеры достигли большого успеха в обеспечении безопасности: только факт присутствия камер видеонаблюдения на объекте может отпугнуть преступника. Но если преступление все же имело место быть, то имеющиеся записи с камер помогут оказать помощь в поимке и опознание злоумышленника. Желание защитить частную собственность и свою семью требует применения самых современных систем безопасности.

Но обеспечение безопасности не единственная область применения систем видеонаблюдения. Большая и малая промышленность все больше нуждается в надежных и автоматизированных средствах контроля и управления технологическими процессами и людьми. При помощи системы видеонаблюдения становится возможным контролировать и управлять многими технологическими и производственными процессами, особенно теми, где нет прямого контроля человеком[1].

В последние 3 года системы видеонаблюдения все больше используются в различных отраслях. Они применяются больницами для постоянного наблюдения за тяжелобольными пациентами, образовательными учреждениями для контроля студентов и учеников, магазинами для наблюдения за покупателями и пресечения попыток краж, муниципальными властями и УВД для наблюдения в общественных местах, в транспорте, местах отдыха и развлечений, банковскими структурами и т.д.

Объект исследования в данной работе – криптографические методы, исследование систем видеонаблюдения и в чем их отличия, какие возможности они дают своему пользователю.

Криптография - это набор методов защиты информационных взаимодействий от отклонений от их нормального, штатного протекания, вызванных злоумышленными действиями различных субъектов, методов, базирующихся на секретных алгоритмах преобразования информации, включая алгоритмы, не являющиеся собственно секретными, но использующие секретные параметры. Исторически первой задачей криптографии была защита передаваемых текстовых сообщений от несанкционированного ознакомления с их содержанием, что нашло отражение в самом названии этой дисциплины, эта защита базируется на использовании "секретного языка", известного только отправителю и получателю, все методы шифрования являются лишь развитием этой философской идеи. С усложнением информационных взаимодействий в человеческом обществе возникли и продолжают возникать новые задачи по их защите, некоторые из них были решены в рамках криптографии, что потребовало развития принципиально новых подходов и методов.

Криптографическими средствами защиты называются специальные средства и методы преобразования информации, в результате которых маскируется ее содержание.

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде[2].

Криптографические методы можно разбить на два класса:

1. обработка информации путем замены и перемещения букв, при котором объем данных не меняется (шифрование);
2. сжатие информации с помощью замены отдельных сочетаний букв, слов или фраз (кодирование).

По способу реализации криптографические методы возможны в аппаратном и программном исполнении.

Для защиты текстовой информации при передачах на удаленные станции телекоммуникационной сети используются аппаратные способы шифрования и кодирования. Для обмена информацией между ЭВМ по телекоммуникационной сети, а также для работы с локальными абонентами возможны как аппаратные, так и программные способы. Для хранения информации на магнитных носителях применяются программные способы шифрования и кодирования.

Аппаратные способы шифрования информации применяются для передачи защищенных данных по телекоммуникационной сети. Для реализации шифрования с помощью смешанного алфавита используется перестановка отдельных разрядов в пределах одного или нескольких символов.

Программные способы применяются для шифрования информации, хранящейся на магнитных носителях (дисках, лентах). Это могут быть данные различных информационно-справочных систем АСУ, АСОД и др. программные способы шифрования сводятся к операциям перестановки, перекодирования и сложения по модулю 2 с ключевыми словами[3].

Особое место в программах обработки информации занимают операции кодирования. Преобразование информации, в результате которого обеспечивается изменение объема памяти, занимаемой данными, называется кодированием. На практике кодирование всегда используется для уменьшения объема памяти, так как экономия памяти ЭВМ имеет большое значение в информационных системах. Кроме того, кодирование можно рассматривать как криптографический метод обработки информации.

Литература

1. Бабаш А. В. Криптографические методы защиты информации: учебник для вузов / А. В. Бабаш, Е. К. Баранова. - Москва: КноРус, 2016. — 189 с.: ил., табл. — (Бакалавриат и магистратура).; ISBN 978-5-406-04766-8 (дата обращения: 10.11.2017);

2. Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях — Научный мир, 2004. — 173 с. — ISBN 978-5-89176-233-6 (дата обращения: 10.11.2017);

3. Мао В. Современная криптография: Теория и практика —М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6 (дата обращения: 10.11.2017).