УДК 681.5

МНОГОФУНКЦИОНАЛЬНАЯ СИСТЕМА ЗАЩИТЫ ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Докиенко С.Ю.
к.т.н., доцент каф. КСУ Великий В.И.
Одесский Национальный Политехнический Университет, УКРАИНА

АННОТАЦИЯ. В статье представлено описание трёх видов защиты банковской организации: защита информации от несанкционированного доступа с помощью симметричного шифрования, противопожарная система защиты и защита от несанкционированного проникновения в помещение.

Введение. Банковская деятельность всегда связана с риском, возможной утечкой информации, наличием внутренних и внешних угроз. Разработка многофункциональной системы защиты связана с четким разбиением ее на несколько частей. При выборе принципа защиты, необходимо всегда рассматривать новейшие варианты, так как постоянно возрастает умение и изощренность взломщиков защиты.

Цель работы. Целью работы является рассмотрение методов информационной, противопожарной защиты и защиты от несанкционированного проникновения на объекты финансовой организации с применением современных аппаратно-программных технологий.

Основная часть работы. Систему защиты финансовой организации разделяют на три основные категории – информационную, противопожарную безопасность и защиту от несанкционированного проникновения на объект. Рассмотрим более детально каждую из них.

Информационная безопасность банка должна обеспечивать высокую надежность работы компьютерных систем даже в случае нештатных ситуаций [2]. Рассмотрим на рисунке 1 пример одного из наиболее применяемых видов шифрования, используемого для защиты информации.

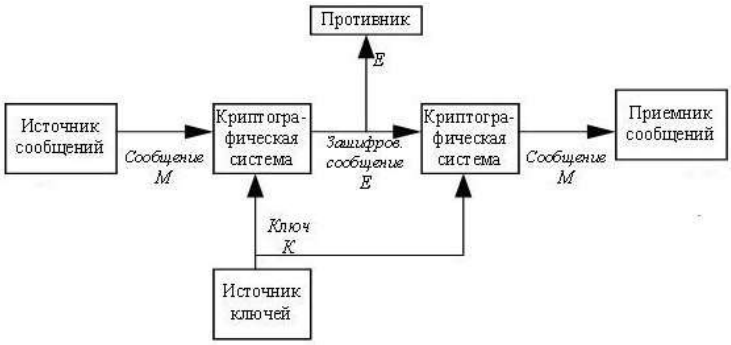

Рис.1 – Общая структура системы, использующей симметричное шифрование

Если M – сообщение, K – ключ, а E – зашифрованное сообщение, то можно записать:

$$E = f(M,K) \quad (1)$$

Зашифрованное сообщение E является некоторой функцией от исходного сообщения M и ключа K. Используемый в криптографической системе метод или алгоритм шифрования и определяет функцию f в приведенной выше формуле.

Важным видом системы защиты является противопожарная безопасность. Основными элементами противопожарной сигнализации являются датчики дыма - ионизационные, оптические и аспирационные [1], потому что тепловые датчики дают сбои в летнее время. На рисунке 2 показан аспирационный дымовой датчик, довольно надежный и достоверный.

Принцип работы датчика заключается в том, что через специальный аспиратор воздух всасывается в систему заборных труб. На первом этапе воздушная проба очищается от пылинок. После прохождения фильтров заборный воздух попадает в измерительную камеру с лазерным излучателем, который просвечивает и анализирует его. Приемник выдает сигнал о задымлении.

Рис. 2 – Принцип работы аспирационного датчика

Третьей обязательной категорией является защита от несанкционированного доступа на объект. Для этого применяются камеры наблюдения, датчики движения и присутствия. Рассмотрим на рисунке 3 структурную схему камеры видеонаблюдения. Чувствительный элемент извещателя представляет собой двухплощадный пироприемник. Тепловое излучение воспринимается чувствительным элементом и фокусируется линзой Френеля. Пироприемник преобразует тепловое излучение из зоны обнаружения в электрический сигнал.

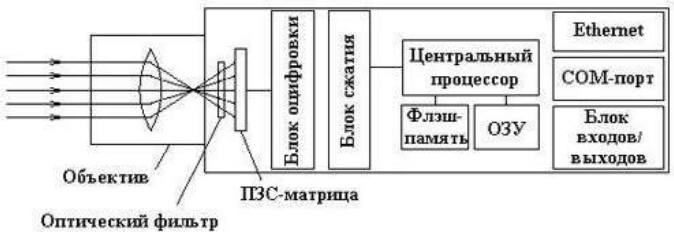

Рис.3 – Структурная схема камеры видеонаблюдения

ОЗУ необходимо для временного хранения информации, флэш-память хранит редко изменяемые данные, центральный процессор производит преобразование электронных зарядов, полученных с матрицы, в цифровой формат, сетевой интерфейс необходим для передачи сформированного, сжатого видеоизображения по локальной сети или интернету.

При внешних условиях недостаточного освещения или даже при полной темноте инфракрасная подсветка обеспечит разборчивое, четкое изображение.

Объектив видеокамеры воспроизводит изображение, увеличенное или сфокусированное, что зависит от фокусного расстояния и глубины резкости. При установке камеры необходимо учитывать угол обзора при видеонаблюдении. Фокусное расстояние определяется по формуле

$$f = \frac{R*A}{L} \quad , \qquad (2)$$

где f –фокусное расстояние, R–расстояние до объекта, A – размер матрицы, L–размер объекта.

Выводы. В статье рассмотрены методы информационной, противопожарной защиты и защиты от несанкционированного проникновения на объекты финансовой организации с применением современных аппаратно-программных технологий. Реалии сегодняшнего дня показывают, что из перечисленных трех направлений защиты нельзя выделить главную или второстепенную. Поэтому любая организация, претендующая на солидность, должна тратить на каждое из направлений не менее 30% - 35% средств из соответствующей статьи расходов. Из них для защиты информации на программное обеспечение расходуется 20% - 25% средств. Столько же средств расходуется на аппаратуру по противопожарной защите и на защиту внешнего и внутреннего периметра.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Михайлов Ю.И. Пожарная безопасность учреждений соцобслуживания М: Альфа-Пресс,2013. -120 с.
2. Родичев Ю.В. Нормативная база в области информационной безопасности П: Питер-Пресс, 2017-256 с.