ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ СИСТЕМЫ ПРЕДРАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ И УПРАВЛЕНИЕ ДОСТУПОМ НАЛОЖЕННЫМИ КОДАМИ

С.Б. САЛОМАТИН, Т.А. БАЙКАЧЕВА, И.А. ФОМЕНКОВА

Сеть специального назначения состоит из нескольких центров и абонентов, связанных между собой каналами связи.

Система предраспределения ключей использует метод общих ключей. Методика шифрования оперирует общими ключами шифрования, имея в наличие информационные группы, состоящие не менее чем из трех процессоров, которые эксплуатируются несколькими абонентами. Процессоры реализуют алгоритмы:

- создания временных интервалов;
- секретности и пересылка его адресату;
- общих ключей внутри группы, которые не доступны абонентам другой группы.

Заложенная в алгоритме предраспределения ключей информация разбивается на подмножества таким образом, чтобы при совместной работе нескольких абонентов имеется возможность определить ключи полностью

Алгоритм преобразования идентификаторов осуществляет преобразование с помощью случайной однонаправленной функции. При кодовом преобразовании средняя величина расстояния Хемминга между двумя случайно выбранными словами должна составлять половину наибольшего кода, а каждый знак кода внутри слова функционально связан с информацией входа.

Для управления доступом используется наложенный код, и модель дизъюнктивного канала множественного доступа (ДКМД). Рассматривается каскадный код с постоянным весом. В качестве внешнего кода используется код Рида-Соломона (РС-код), а в качестве внутреннего — ортогональный код. Под декодером наложенного кода понимается отображение последовательности, сформированной в ДКМД на множество кодовых слов из данного наложенного кода. Рассматривается алгоритм

сокращенного перебора, использующий свойство быстрого поиска переданных элементов поля и структуры РС-кодов. Алгоритм позволяет осуществить успешное декодирование, когда переданное по ДКМД множество превосходит расчетный порядок кода.