доступ к ресурсам файлового сервера, к принтерам и другим устройствам в доменной сети с контроллером домена и службой каталогов Active Directory осуществлялся при помощи списков доступа Access Control List (ACL), а для более защищенных ресурсов с применением шифрования – службы управления правами (Rights Management Services). С помощью этих средств администратор мог назначить права доступа к папкам, файлам для определенного пользователя, используя только его членство в определенной группе безопасности домена. При большом количестве общих папок и других ресурсов приходилось создавать большое количество групп в домене.

Динамический контроль доступа Dynamic Access Control Windows Server (DAC) создает дополнительный уровень безопасности, применение этой технологии позволяет сконфигурировать права доступа к папкам и файлам, учитывая не только членство в группах безопасности, но и другие параметры пользователей и устройств, зафиксированные в Active Directory сервера, например: Department (Отдел), Country (Страна) и т. п. Технология базируется на трех основных понятиях: классификация документов (на основе свойств файлов, например, местоположение файла); утверждение (сформулированное условие, которое соответствует значениям атрибута пользователя или компьютера); аудит (политика аудита позволяет получить информацию о попытках доступа к конфиденциальной информации).

**Литература**

1. Microsoft Windows Server 2012. Полное руководство / Р. Моримото [и др.]. М.: ООО «И.Д. Вильямс», 2013. 1456 с.

2. Windows Server 2012 R2. Полное руководство / М. Минаси [и др.]. М.: ООО «И.Д. Вильямс», 2015. 960 с.

## ОДНОСТОРОННЯЯ ФУНКЦИЯ НА ОСНОВЕ ТЕОРИИ СЛУЧАЙНЫХ РЕШЕТОК

С.Б. Саломатин

Основные задачи, связанные с построением односторонних функций на основе теории решеток связаны с решением двух задач. Первая – задача декодирования на абсолютном расстоянии $d$. Если $d$ больше определенной величины, то решение гарантированно существует. Вторая задача связана с декодированием на граничном расстоянии: если решение существует, то оно единственно. Решение этих двух задач на случайных решетках может быть сформулировано в рамках задачи инвертирования функции $f(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod p$.

Определим решетку $L$ как подгруппу векторов по модулю $p$ целых чисел. Дуальную (ортогональную) к ней решетку обозначим как $D$. Конечное множество точек $Q$ решеток образуют множество с координатами в $\{0, 1, \ldots, p-1\}$.

Дуальные решетки могут быть использованы для получения различных (эквивалентных) конструкций односторонних функций. Образуем решетку $L(\mathbf{A})$ из случайной матрицы $\mathbf{A}$ массива целых чисел с модулярной операцией. Тогда решение двух основных задач криптографических решеток в рамках выбора случайной точки $\mathbf{v}$ и вектора ошибки $\mathbf{x}$ и получения целевого показателя $\mathbf{t} = \mathbf{v}+\mathbf{x}$. Решетки периодичны по модулю $p$, все векторы редуцированы по модулю $p$ и точка решетки может быть выбрана из массива конечного множества $L \bmod p$ с равномерным распределением. Случайная точка представляется как $v = \mathbf{A}\mathbf{s} \bmod p$. Односторонняя функция имеет вид A’$\mathbf{s} + \mathbf{x} \bmod p$, где вектор $\mathbf{s}$ принадлежит векторному массиву целых чисел. Односторонняя функция имеет два входа: вектор $\mathbf{s}$ из массива случайных чисел с равномерным распределением и вектор ошибки $\mathbf{x}$, соответствующий заданной функции $f$. Функция становится свободной от коллизий при достаточно большом размере вектора $\mathbf{x}$.

Односторонняя функция на основе случайных решеток может быть использована в схемах сетевого кодирования и системах связи.