ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

УДК 004.414

Пороговое разделение файлов на основе битовых масок: идея и возможное применение

Н. С. Могилевская
(Донской государственный технический университет),
Р. В. Кульбикаян
(Ростовский государственный университет путей сообщения),
Л. А. Журавлёв
(Донской государственный технический университет)

Предлагается новый метод порогового разделения файла любого формата на n частей таким образом, чтобы для его корректного восстановления было необходимо собрать не менее k(<n) частей. Предложенный метод может быть использован для децентрализованного хранения файлов, для передачи файлов по многоканальным сетям, а также для защиты от несанкционированного доступа к информации, содержащейся в файле.
Ключевые слова: *пороговое разделение секрета, метод битовых масок, безопасность файлов, децентрализованное хранение файлов, передача файла по многоканальной системе связи.*

Введение. Идея данной работы родилась на стыке трёх задач, для решения которых в том или ином виде используется разделение данных на части для повышения уровня их сохранности. Так, первая задача состоит в предохранении секретной информации (ключей) от потери, разделении ответственности за принятие решения и предотвращении атак, связанных с человеческим фактором, таких, как подкуп, шантаж, захват людей, имеющих отношение к секретной информации. Решается эта задача с помощью пороговых схем разделения секрета, разработанных в теории криптографических протоколов. (k, n)-пороговым протоколом разделения секрета называют распределённый алгоритм, в котором некоторый числовой секрет N разделяется на n частей-долей и распределяется между участниками таким образом, чтобы любые k участников, собравшись вместе, могли восстановить секрет N, а любые (k – 1) участников ничего не могли узнать о секрете [1, 2, 3]. На сегодняшний день существует большое количество схем разделения секрета, например [1, 3]. Наиболее известной, пожалуй, является (k, n)-пороговая схема Ади Шамира, в основе которой лежит известный алгебраический факт, что для восстановления всех коэффициентов полинома $f(x)$ степени $k - 1$ необходимо знать значение $f(x)$ в k различных точках. Согласно схеме Шамира, используются полиномиальные уравнения в конечном поле F_p, где p — простое число, больше количества возможных долей n и больше любого возможного секрета [3]. К подготовительной части этой схемы относится генерация полинома $f(x)$ степени $k - 1$ со случайными коэффициентами из F_p, такого, что значение секрета равно $f(0)$. Долей секрета участника j ($j = 1, \ldots, n$) схемы является пара вида (x_j, $f(x_j)$), где $x_j = 1, \ldots, p - 1$. Для восстановления секрета $f(0)$, согласно (k, n)-пороговой схеме Шамира, используется интерполяционная формула Лагранжа. Ещё одна популярная схема предложена Джорджем Блэкли [3], в которой секретом является одна из координат точки Q в k-мерном пространстве, а долями секрета являются уравнения плоскостей, пересекающихся в Q. Для восстановления секрета не-