$R=\{r_1, r_2, r_3\}$, где r_1 — вариант реализации средств; r_2 — расположение средств; r_3 — функции средств.

Предлагается в одном из подмножеств отразить социально-психологические качества потенциального нарушителя: замкнутость или общительность, воля или нерешительность, авантюризм, прагматизм, карьеризм и др. Это позволит создать гипотетическую модель наиболее опасного нарушителя и выделить так называемую "группу риска".

Синтез моделей проводится с использованием аппарата логики высказываний.

Расширение номенклатуры классифицирующих признаков позволит детализировать модель нарушителя и получить более достоверные оценки вероятного направления, характера и риска возможного несанкционированного доступа.

ЗАДАЧА ИДЕНТИФИКАЦИИ АТАК В СРЕДСТВАХ АУДИТА БЕЗОПАСНОСТИ

Е.П. МАКСИМОВИЧ

В соответствии со стандартом СТБ 34.101.2-2001 (ИСО/МЭК 15408-2) средства аудита безопасности должны обнаруживать возможные нарушения безопасности на основе идентификации определенных правил, знаковых событий; известных сценариев проникновения; несоответствия текущей деятельности пользователя ранее применяемому профилю использования системы. Правила, знаковые события и профили стандартного поведения представляют собой некоторые шаблоны или экспертные правила, каждому из которых соответствуют нечеткое слабо формализуемое множество возможных реализаций. В таких условиях возникает нетривиальная задача идентификации наблюдаемых действий, выраженных в некоторых низкоуровневых сигналах относительно заданных эталонных описаний.

Один из возможных подходов к решению указанной задачи идентификации состоит в использовании распознавания с обучением.

Каждая атака представляется выборкой возможных реализаций, которые образуют один или несколько кластеров близких (в смысле заданной функции) ситуаций. Идентификация ситуации сводится к оценке ее возможной принадлежности одному из полученных кластеров. Если расстояние ситуации до ближайшего кластера меньше заданного порогового значения, то принимается решение о реализации соответствующей атаки. Для определения значения порога можно использовать контрольную выборку. В качестве критерия близости предлагается использовать правило типа "ближайшего соседа" либо близость к эталону кластера, заданному, например, в виде дизъюнктивной нормальной формы.

РАНДОМИЗАЦИОННЫЕ ПРЕОБРАЗОВАНИЯ С АЛФАВИТОМ БОЛЬШОЙ МОЩНОСТИ

В.В. ЗАХАРОВ

Известно, что одним из приемов, разрушающих частотные свойства исходного текста является рандомизация. В процессе рандомизации буквам алфавита исходного текста случайным образом ставятся в соответствие буквы алфавита рандомизированного текста. При этом если мощность алфавита рандомизатора незначительно превышает мощность алфавита исходного текста, то такой шифр может быть легко вскрыт.

Доклад посвящен синтезу и анализу рандомизационных преобразований с большой мощностью алфавита рандомизатора.

Показано, что такие рандомизаторы при мощности алфавита рандомизации $L \to \infty$ обеспечивают бесконечную энтропию криптограммы и, соответственно, полную статистическую независимость криптограммы от исходного текста. При этом возможно получение различной степени приближения к полной статистической независимости исходного и зашифрованного текстов путем использования рандомизатора с ограниченным, достаточно большим полем рандомизации.

Дана численная оценка мощности алфавита рандомизатора, при которой достигается практическая статистическая независимость исходного текста и криптограммы.

Приведена методика синтеза рандомизаторов с большой мощностью алфавита рандомизации на основе кусочно-линейных разрывных функций. Показаны возможные подходы к анализу стойкости таких рандомизаторов.

МЕТОД МНОГОКАНАЛЬНОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ И ЕГО ПРИМЕНЕНИЕ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Ю.В. ВИЛАНСКИЙ

В 1999 году в заявке PCT /BY99/ 00005 был предложен метод преобразования данных, в котором исходный текст преобразуется в два или более выходных потока. Особенностью метода является циклический характер получения составляющих выходных потоков, что позволяет распределять их совокупности, каналам передачи или использовать как дополнительные степени свободы в различных системах. При этом, по крайней мере, один из выходных потоков можно сделать достаточно малым.