инциденты, связанные с нарушением контроля целостности данных, хранимых на серверах предприятия.

Литература

1. Guide to Computer Security Log Management [Электронный ресурс]. – Электронные данные. – Режим доступа : http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

СТАТИСТИЧЕСКАЯ ПРОВЕРКА СЛУЧАЙНОСТИ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ТЕСТАМИ NIST DRAFT SP 800-90B

Е.В. Ставер

Одной из актуальных задач криптографии является задача исследования статистических свойств бинарных последовательностей, используемых для создания ключей криптографических алгоритмов. Разработан программный комплекс проверки последовательностей на случайность по стандарту DRAFT 800-90b. Приведены результаты разработки программного комплекса и тестирования, с помощью его четырех последовательностей последовательности bits.01, bits.02, calif.bit, germany.bit, тестами по критерию «хи-квадрат» и тестом проверки на коллизии. Проверка по критерию «хи-квадрат» позволит узнать, насколько созданный реальный ГСЧ близок к эталону ГСЧ, т.е. удовлетворяет ли он требованию равномерного распределения. Тест на коллизии измерит оцениваемое время до первой коллизии в выборке.

Цель статистики коллизий – оценка вероятности наступления наиболее желаемого состояния, основываясь на времени коллизий.

УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ, ПРОБЛЕМЫ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

Л.Л. Утин, А.Р. Мацылевич

В целях обеспечения защищенности информационных ресурсов должна быть создана система защиты информации (СЗИ), к которой предъявляется ряд требований [1, 2]. Важным условием функционирования СЗИ, как системы, обладающей целевой функцией, является осуществление эффективного управления. Одной из особенностей управления защитой информации является то, что в основном объекты управления имеют техногенную природу, а субъекты управления — антропогенную. Данный факт в большинстве своем отрицательно сказывается на адекватном функционировании СЗИ. Кроме того, одним из критически важных факторов, оказывающим воздействие на защиту информации, является так называемый «человеческий фактор», который особенно сильно влияет на процессы управления защитой информации. Одним из путей минимизации влияния «человеческого фактора» и повышения эффективности СЗИ в целом, является организация управления защитой информации.

Проведенный анализ возможностей существующих технических средств и систем защиты информации свидетельствует о том, что они в основном являются локальными и выполняют ограниченные задачи (системы защиты от несанкционированного доступа, системы обнаружения и предотвращения вторжений, системы анализа защищенности сети и др.). При этом функции единого управления в масштабах всей сети (корпоративной сети) не реализуются.

О существующих при этом некоторых проблемах и возможных путях их решения ведется речь в докладе.

Литература

1. Защита информации. Основные термины и определения: СТБ ГОСТ Р 50922-2000. – Введ. 01.01.2001 – Мн. : Госстандарт, 2001. - 6 с.

2. О некоторых вопросах технической и криптографической защиты информации: приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 30 авг. 2013 г., № 62 // [Электронный ресурс].