

Для реализации метода необходимо разработать программы мониторинга и управления. Программа управления должна иметь функцию задания маски имен отслеживаемых файлов, а также функцию графического отображения маршрута перемещений. Модуль мониторинга должен устанавливаться на конечных ПК локальной сети и следить за изменениями целевых файлов по предложенной выше схеме.

#### **Литература**

1. *Алиев А.Т.* Разработка моделей, методов и алгоритмов перспективных средств защиты информации в системах электронного документооборота на базе современных технологий скрытой связи: дис. ... канд. техн. наук: 05.13.13/А. Т. Алиев; Ростов-на-Дону, 2008 – 216 с

### **ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ**

А.П. Жук, А.А. Гавришев, В.А. Бурмистров

Сегодня в мире основными технологиями беспроводной передачи информации являются GSM, 3G, HSPA+/HSPA+ Advanced (4G), WiMAX, LTE (4G). В последнее время данные технологии активно внедряются во многие системы передачи информации, например в охранно-пожарные системы безопасности. Однако, в силу уязвимости беспроводного канала связи для несанкционированного доступа актуальным является вопрос обеспечения его защищенности. В настоящее время защищенность радиоканала, в основном, обеспечивается средствами криптографической защиты информации (СКЗИ). СКЗИ имеют следующие минусы: дороговизна, значительное время выполнения команд шифрования-расшифрования, изученность основных алгоритмов. Альтернативным методом защиты радиоканала является применение генераторов стохастических ортогональных сигналов [1], заключающимся в том, что для передачи сообщений, сменяемых от одного информационного символа к другому, предлагается использовать сформированные стохастическим образом ортогональные системы сигналов, описываемые собственными векторами диагональной симметрической матрицей  $A$  размерностью  $N$ . При этом используется свойство ортогональности собственных векторов, заключающееся в том, что собственные векторы, соответствующие различным собственным значениям нормального оператора, попарно ортогональны. Данный метод отличается увеличенным числом структур сигналов и уменьшенной вероятностью их раскрытия за счет расширения диапазона  $n$  возможных значений диагональных коэффициентов матрицы  $A$ .

#### **Литература**

1. *Жук А.П. и др.* Способ передачи информации на основе хаотически формируемых ансамблей дискретных многоуровневых сигналов / Патент РФ № 2428795, 10.09.2011.

### **ПРОТОКОЛОВ ЗАЩИТЫ ИНФОРМАЦИИ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ ПРЯМЫХ**

А.М. Захаревич

В последнее время все больше и больше внедряются в нашу повседневную жизнь информационные технологии, пытаясь захватить в ней все: от важнейших государственных проектов до решения обычных бытовых проблем. Вместе с огромной пользой и, казалось бы, неограниченными возможностями новые технологии приносят и новые проблемы. Одной из них является проблема защиты информации от несанкционированного посягательства теми, кто доступа к этой информации иметь не должен. В связи с этим почти одновременно с развитием информационных и компьютерных технологий начали развиваться и технологии защиты информации, развитие которых с некоторой точки зрения гораздо более критично, чем развитие непосредственно информационных технологий. Ведь с совершенствованием систем защиты, совершенствуются и методы взлома, обхода этих защит, что требует постоянного пересмотра и увеличения надежности защиты информации.

Практически любая "современная" криптосистема может быть "переложена" на эллиптические кривые, но не для всех схем это дает выигрыш в стойкости. Например, для

системы RSA и родственных ей систем, основанных на сложности задачи факторизации, это не усиливает схему. В то же время для схем, основанных на сложности задачи логарифмирования в дискретных полях, переход на эллиптические кривые позволяет существенно увеличить стойкость. Обусловлено это тем, что при надлежащем выборе параметров кривой задача логарифмирования в группе точек кривой существенно сложнее задачи логарифмирования в мультипликативной группе исходного поля. По указанной причине в настоящее время происходит массовый перевод асимметричных криптосистем, основанных на сложности задачи логарифмирования в дискретных полях, на эллиптические кривые.

## **КОНЦЕПЦИЯ ЗАЩИТЫ ИНФОКОММУНИКАЦИЙ ОТ КИБЕР-УГРОЗ**

**А.Ю. Зинченко, В.Ю. Цветков, Алби Гарби Хушам Абдулхусейен Худайр**

Спектр современных угроз информационной безопасности и время их проведения изменчив. Атаки осуществляются за минуты, в то время как обнаружение занимает недели и месяцы. Для противодействия угрозам разработана концепция, которая реализуется на всех элементах (сеть, мобильные устройства, виртуальные машины, облака и др.). Концепция состоит из следующих частей: действия до атаки (контроль, усиление), во время атаки (обнаружение, блокирование) и после (устранение). На каждом участке необходимо применять соответствующие технологии. Так, на участке до атаки необходимо применять такие технологии как: Firewall, App Control, VPN, IAM/NAC. Во время — IPS, Anti-Virus, Email/Web Security. После атаки — IDS, FPC, Forensics, SIEM. Важными составляющими данной концепции являются: корреляция угрозы с устройством в сети, и необходимость агрегирования многих источников данных для определения угрозы (определения атакующего и его цели). Данная возможность реализована посредством протокола NetFlow. В рамках данной концепции, защита сетевой среды должна состоять из трёх частей: глубокого просмотра в точках анализа (идентификация/блокировка приложений и файлов, траектория файлов), защита доступа к сети и инфраструктуре (видимость пользователей и устройств, авторизация), а также широкий обзор на всех сетевых уровнях (сбор данных по всему трафику, обнаружение подозрительной и аномальной активности). Поскольку все объекты соединяются друг с другом различными взаимоотношениями, образуя единый граф, концепция подразумевает изменение тактики защитника, в частности, переход от анализа списков, к анализу графов.

## **МЕТОДЫ И ПРОГРАММНЫЕ СРЕДСТВА ИНТЕРАКТИВНОЙ ВИЗУАЛИЗАЦИИ МЕХАТРОННЫХ СИСТЕМ**

**Г.А. Zubov, В.В. Поляковский**

Целью исследования является анализ существующих средств и методов интерактивной визуализации трехмерных сцен, подходов к взаимодействию между объектами трехмерной сцены. В ходе работы были рассмотрены популярные программные системы моделирования, использующиеся в различных областях промышленности, а также применяемые в них подходы. Такой анализ позволит уточнить требования для разработки специализированной системы интерактивной визуализации, а также на раннем этапе выявить ошибки в реализации. Объектами исследования являются программные продукты, используемые на различных уровнях разработки трехмерных интерактивных сцен. Это, с одной стороны, и готовые продукты, различные CAD/CAM системы, так и программные библиотеки для разработки трехмерных графических приложений. Их недостатком является достаточно низкие возможности по модифицированию используемых трехмерных моделей. Среди наиболее популярных в конструировании графического программного обеспечения были рассмотрены такие программные библиотеки, как OpenGL, DirectX, XNA Framework. Все они достаточно функциональны для конструирования трехмерных сцен, но наибольшим удобством именно для интерактивных систем обладает XNA Framework.