Рефераты статей тома № 8 Трудов научно-технической конференции кластера пензенских предприятий, обеспечивающих

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ворона Ю.В., Иванов А.И. **Пакет российских биометрических стандартов как одна из предпосылок устойчивого развития информационного общества.** Пенза-2012, Том 8, с. 3-7, Трудов конференции «БИТ», УДК: 681.322.

В работе рассматривается гипотеза периодической утраты устойчивости развивающимся обществом. Отмечается, что переход к информационному обществу сопровождается утратой его устойчивости. Возврат к устойчивому развитию возможен через массовое использование полицейской биометрии, активно создаваемой США, и через массовое использование гражданской биометрии, активно создаваемой Россией. Полицейская биометрия общественного контроля и гражданская биометрия защиты цифровых прав личности дополняют друг друга. Даны ссылки на стандарты по этим двум ветвям технического развития.

Надеев Д.Н. **Синтез функции для вычисления вероятности пропуска «Чужого» по статистическим параметрам зависимых кодов-откликов «Чужой».** Пенза-2012, Том 8, с. 8-9, Трудов конференции «БИТ», УДК: 681.322.

В работе построена трехмерная функция плотности вероятности появления кодов с зависимыми разрядами, соответствующая модифицированной схеме испытаний Бернулли. Приведена программа для некоммерческой среды моделирования SMath Studio, позволяющая приближенно оценивать вероятность ошибочного пропуска «Чужого», путем задания длины кода, средней вероятности состояний разрядов кода, среднего модуля коэффициентов корреляции между разрядами кодов.

Мацкевич А.Г., Егоров Н.С. **Сопоставительный анализ вычислительной сложности существующих методов факторизации длинных чисел.** Пенза-2012, Том 8, с. 10-13, Трудов конференции «БИТ», УДК: 681.322.

Статья посвящена методам криптоанализа несимметричных криптографических систем, основанных на сложности задачи факторизации длинных чисел. В ней рассмотрены оценки временной сложности таких методов как: квадратичного решета, Ленстры и решета числового поля. В статье предложены их модификации, которые помогут уменьшить вычислительную сложность методов или сократить время факторизации через распараллеливание вычислений.

Пустыгин А.Н. **Оценка показателей роста сложности задач анализа и комментирования программных кодов.** Пенза-2012, Том 8, с. 14-17, Трудов конференции «БИТ», УДК: 681.322.

В работе обосновывается важность для программной индустрии механизмов автоматического комментирования исходных текстов программ. Показан экспоненциальный рост сложности задачи формальной нотации знаний разработчика о ПО в форме эквивалентной исходному тексту. Предлагается решение задач автоматического исследования исходных текстов ПО с помощью специализированных программных инструментов.

Куликов С.В. **Оценка энтропии биометрических образов через переход к дискретному представлению с ассиметричным распределением меры Хемминга.** Пенза-2012, Том 8, с. 18-21, Трудов конференции «БИТ», УДК: 681.322.

Показано, что удается вычислять энтропию непрерывных высокоразмерных биометрических образов, если воспользоваться промежуточной дискретизацией каждого из контролируемых биометрических параметров. При таком подходе распределение меры Хемминга оказывается существенно асимметричным, однако его можно представить

смесью нормальных законов. Для вычислений достаточно учесть только первый компонент смести нормальных законов. Оценка параметров первого компонента смеси нормальных законов примитивна.

Майоров А.В. **Введение дополнительной избыточности для защиты параметров преобразователей биометрия-код от попыток исследования.** Пенза-2012, Том 8, с. 22-26, Трудов конференции «БИТ», УДК: 004.424.47: 004.056.53.

Предложено несколько вариантов усиления хеширующих свойств нейросетевых преобразователей биометрия-код. Все предложенные модификации связаны с введением дополнительной информации. Показано, что каждая из предложенных модификаций дает эффект размножения ошибок при попытке реализовать атаку направленного подбора биометрических образов.

Язов Ю.К., Майоров А.В. **Язык описания схем работы преобразователя биометрия-код для проведения сертификационных испытаний.** Пенза-2012, Том 8, с. 27-31, Трудов конференции «БИТ», УДК 004.434: 004.006.

Рассматривается проблема синтеза специализированного языка для проведения сертификационных испытаний нейросетевых преобразователей биометрия-код. Если тестируемое средство биометрической защиты выполнено с интерфейсами по ГОСТ Р 52633.4-2011, то упростить сертификацию удается, применяя специализированный язык описания схем работы преобразователей биометрия-код. В новом языке появляются такие операторы как «создать нейросеть», «обучить», «тестировать». Отличие нового языка от иных формальных языков состоит в его ориентации на описание искусственных нейронных сетей и нечетких биометрических данных.

Андреев Д. Ю. **Сокращение затрат на нечеткую взаимную адресацию биометрических образов через использование взвешенной меры Хэмминга.** Пенза-2012, Том 8, с. 32-35, Трудов конференции «БИТ», УДК 519.7+621

Показано, что взаимное упорядочивание нечеткой адресации биометрических образов может быть упрощено за счет использования взвешенной меры Хэмминга. Предложено использовать коэффициенты взвешивания пропорциональные стабильности сравниваемых разрядов кода. Если система вырождается и оказывается полностью детерминированной (все разряды кода имеют высокую стабильность), то взвешенная мера Хэмминга становится обычной мерой Хэмминга. За счет ослабления влияния нестабильных разрядов удается снизить длину кодов взаимного упорядочивания до 30%, соответственно снижаются затраты на взаимное упорядочивание нечетких биометрических образов.

Секретов М.В. **Комплексный показатель качества средств нейросетевой биометрической аутентификации.** Пенза-2012, Том 8, с. 36-37, Трудов конференции «БИТ», УДК 57.087.1: 621.391.

Рассматривается ситуация, когда значения ошибок первого и второго рода существенно отличаются у сравниваемых между собой средств аутентификации. Предложено в качестве меры сравнения использовать обратную величину среднего геометрического вероятностей ошибок первого и второго рода. Подобная мера одновременно учитывает оба показателя и дает возможность сравнивать между собой совершенно разные биометрические технологии.

Козачок А.И., Левицкая Ю.А. **Итерационный алгоритм построения оптимальной политики безопасности ТКС.** Пенза-2012, Том 8, с. 38-40, Трудов конференции «БИТ», УДК 681.322.

В работе рассматривается выбор оптимальной политики безопасности на основе использования марковских процессов и итерационного алгоритма – обобщенного метода Ховарда. Метод Ховарда позволяет найти оптимальное решение за небольшое число итераций, каждая из которых состоит из двух процедур: оценивание параметров прибыли и улучшение стратегии. При использовании данного метода нахождение оптимальной стратегии общих марковских процессов принятия решений возможно без классификации состояний на каждой итерации.

Васинев Д.А., Кузнецов А.А. **Моделирование процесса доступа в сеть общего пользования на основе технологии socks.** Пенза-2012, Том 8, с. 41-44, Трудов конференции «БИТ», УДК 681.322.

Моделирование доступа пользователей к внешним информационным ресурсам через Интернет может быть использовано для повышения защищенности ресурсов компьютерной сети при доступе пользователя к информационным ресурсам сети общего пользования. Результат моделирования позволяет рассчитать параметры подсистемы доступа (число промежуточных серверов, задержку и путь прохождения пакетов), которые применяются для доступа к информационному ресурсу в сети общего пользования. Сеть socks серверов позволяет изменять путь прохождения пакетов и точку выхода в сети общего пользования, в момент возникновения угрозы информационной безопасности, осуществлять динамическое изменение параметров на средствах обеспечения информационной безопасности в случае определения в точке выхода угрозы информационной безопасности.

Беляев Д. Л., Нешин Д. В., Байбосын А. Б. **Управление доступом к информационным ресурсам разного уровня доверия.** Пенза-2012, Том 8, с. 45-48, Трудов конференции «БИТ», УДК 681.322.

В работе рассматривается возможность предотвращения утечки информации при подключении автоматизированной системы к мультисервисным сетям разного уровня доверия посредством контроля за процессами и потоками, выполняемыми в операционной системе. Отмечается, что управление доступом может быть реализовано посредством оценки защищённости автоматизированной системы с применением аппарата нечётких множеств и управляемых цепей Маркова.

Фунтиков В.А., Иванов А.И. **Оценка избыточности сильно коррелированных случайных кодов с использованием двухмерной номограммы их энтропии** Пенза-2012, Том 8, с. 49-52, Трудов конференции «БИТ», УДК 519.7; 57.087.1

Рассматривается один из быстрых алгоритмов оценки энтропии коррелированных кодовых последовательностей. Показано, что вычисление энтропии и избыточности этих кодовых последовательностей по Шеннону занимает большой интервал времени. Предложено вычислять среднее значение модулей коэффициентов корреляции между случайно выбранными битами кодов. В этом случае достаточно всего 1000 кодов для вычисления их энтропии и избыточности. Дана двухмерная номограмма связи высокоразмерной энтропии с усредненным модулем вычисленных коэффициентов парной корреляции.

Иванов А.И., Язов Ю.К. **Рост скорости программирования биометрических приложений при использовании специальных языков автоматического обучения искусственных нейронных сетей большой размерности.** Пенза-2012, Том 8, с. 53-55, Трудов конференции «БИТ», УДК 519.7; 57.087.1

Показано, что применение алгоритмов автоматического обучений искусственных нейронных сетей большого размера по ГОСТ Р 52633.5 эквивалентно увеличению

скорости программирования примерно в миллиард раз. Замена ручного программирования на автоматизированное возможно только после появления специализированных языков для связывания нейросетевого подсознания (аналоговой формы представления информации) и полностью детерминированной цифровой части сознания искусственного интеллекта. Создаваемый сегодня язык программирования для биометрических приложений является первой упрощенной версией подобных языков.

Иванов А.И. **Взаимное определение последовательности базовых понятий: данные, информация, знания, сознание, подсознание.** Пенза-2012, Том 8, с. 56-59, Трудов конференции «БИТ», УДК 519.7; 57.087.1

Рассматривается последовательность связанных между собой терминов. Отмечается, что термины должны определяться друг через друга в последовательности их усложнения. Кроме того, должны быть введены уточнения по форме представления данных, информации, знаний, интеллекта. Необходимо разделять между собой аналоговую и цифровую формы представлений данных, информации, знаний, интеллекта. Цифровую часть интеллекта предлагается рассматривать как медленное низко размерное сознание, а аналоговую часть интеллекта предлагается рассматривать как быстрое многомерное подсознание.

Елфимов А.В. **Человеко-машинный алгоритм восстановления сильно зашумленных рукописных изображений букв.** Пенза-2012, Том 8, с. 60-62. Трудов конференции «БИТ», УДК 519.7; 57.087.1

Рассматривается процедура восстановления псевдодинамики воспроизведения рукописных букв путем автоматизированной обработки данных, полученных после по факсу. Показано, что вмешательство человека позволяет верно восстанавливать траекторию движения пера в рамках гипотезы постоянной скорости. Удается работать при уровне шумов много выше уровня полезного сигнала.

Безяев А.В., Фунтикова Ю.В. **Оптимизация параметров хэш-кодов, осуществляющих обнаружение и корректирование ошибок в биометрических преобразователях.** Пенза-2012, Том 8, с. 76-80, Трудов конференции «БИТ», УДК 519.7; 57.087.1

В работе рассматриваются коды не обладающие избыточностью, используемые нейросетевыми биометрическими преобразователями. Показана проблема необходимости увеличения исправляющей способности кодов, обнаруживающих и исправляющих ошибки по усеченным хэш-функциям. Предлагается вариант обработки биометрического кода, позволяющий исправлять в 5 раз большее количество ошибок без увеличения вычислительных затрат.