МЕТРИКИ ДЕСТРУКТИВНОГО КОНТЕНТА НА ВИДЕОХОСТИНГЕ YOUTUBE

А.Г. Остапенко, В.Е. Кунавин, В.С. Сидельникова, О.А. Остапенко

В данной статье рассмотрено влияние деструктивного контента на платформе, предоставляющей возможность просмотра и загрузки медиаконтента в формате видеороликов. Особое внимание уделено мониторингу региональных каналов на основе метрик, помогающих выявлению деструктивного контента на платформе YouTube.

Ключевые слова: сеть, медиа, YouTube, деструктивный контент.

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ ОРГАНИЗАЦИИ, ПОДКЛЮЧЕННОЙ К СЕТИ ИНТЕРНЕТ

О.Н. Чопоров, Е.Р. Нежельский, В.И. Белоножкин, Л.В. Паринова

Предлагается последовательность алгоритмов и процедур (формирование численных оценок рисков на основе методов экспертного оценивания, выбор оптимального, с точки зрения соотношения стоимости и эффективности, комплекса защитных мер на основе метода анализа иерархий), направленных на решение задачи выбора эффективных защитных мер в рамках системы управления рисками организации.

Ключевые слова: система управления, риски организации, анализ рисков, план обработки рисков.

ОБНАРУЖЕНИЕ ПОДМЕНЫ ПОЛЬЗОВАТЕЛЕЙ В КОМПЬЮТЕРНЫХ СИСТЕМАХ НА ОСНОВЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

М.В. Дагаева, Д.В. Катасёва, А.С. Катасёв

В данной статье рассматривается проблема обнаружения подмены пользователей в компьютерных системах. Для решения данной проблемы актуализируется необходимость аутентификации пользователей по их биометрическим признакам на основе нейронной сети. При построении модели производилась оценка информативности входных признаков на основе алгоритма DEL. Построенная модель позволила эффективно решить задачу обнаружения подмены пользователей в компьютерных системах.

Ключевые слова: нейронная сеть, биометрия, идентификация и аутентификация, корреляционный анализ, подмена пользователя.

ПРОГНОЗИРОВАНИЕ ВЫХОДНЫХ ПАРАМЕТРОВ НЕЙРОСЕТЕВОГО ПРЕОБРАЗОВАТЕЛЯ "БИОМЕТРИЯ - КОД ДОСТУПА" НА ОСНОВЕ ЭЛЕКТРОЭНЦЕФАЛОГРАММЫ

С.М. Гончаров, А.Е. Боршевников

В статье рассматриваются выходные параметры модели нейросетевого преобразователя «Биометрия - код доступа» на основе электроэнцефалограммы. Приводится прогноз выходных значений вероятностей ошибок первого и второго рода модели нейросетевого преобразователя «Биометрия - код доступа» на основе электроэнцефалограммы.

Ключевые слова: нейросетевой преобразователь «биометрия – код доступа», восстановление ключа, электроэнцефалограмма, P300, биометрическая аутентификация.

ВЫЯВЛЕНИЕ DDOS-АТАК НА ОСНОВЕ НЕЙРОСЕТЕВОЙ ТЕХНОЛОГИИ

Ю.Н. Воробьева, Д.В. Катасёва, А.С. Катасёв

В данной статье рассматривается проблема выявления DDoS-атак. Анализируются основные механизмы запуска и методы выявления DDoS-атак. В качестве эффективного инструмента выявления DDoS-атак предложено использовать нейронную сеть. Для ее построения была проведена подготовка исходных данных, разработка структуры нейронной сети, ее обучение и оценка адекватности. Построенная нейронная сеть справляется с задачей выявления DDoS-атак.

Ключевые слова: DDoS-атака, информационная безопасность, нейронная сеть.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПРОЦЕДУРЫ ПЕРЕМЕЖЕНИЯ НА КАЧЕСТВО ИНФОРМАЦИОННОГО ОБМЕНА С ИСПОЛЬЗОВАНИЕМ КАСКАДНОГО ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

В.А. Свищев, В.Е. Дидрих, В.А. Гриднев, И.В. Дидрих

В работе проведен анализ необходимости применения перемежения при использовании каскадного помехоустойчивого кодирования в ДКМВ канале передачи данных. Сделан вывод об ограниченности применения перемежителя для внешнего помехоустойчивого кода и о необходимости его применения для внутреннего кода.

Ключевые слова: каскадный код, перемежение, помехоустойчивое кодирование.

ЧАСТОТНО-ГЕНЕТИЧЕСКИЙ МЕТОД ОЦЕНКИ СТОЙКОСТИ ШИФРОВ МОНОАЛФАВИТНОЙ ЗАМЕНЫ

А.Д. Кабиров, Д.В. Катасёва, А.С. Катасёв

Данная статья посвящена оценке стойкости шифра моноалфавитной замены. Для этого разрабатывается система, в которой к зашифрованному тексту применяется сначала частотный анализ, а затем генетический алгоритм. Описываются различные параметры генетического алгоритма, способные повлиять на эффективность работы системы. Оценивается эффективность реализации разработанной системы в зависимости от различных параметров генетического алгоритма. Делается вывод о стойкости шифра моноалфавитной замены.

Ключевые слова: симметричные шифры, моноалфавитная замена, частотный анализ текста, генетический алгоритм, криптоаналитическая атака.

ОБЩАЯ СХЕМА РАЗРАБОТКИ ЯЗЫКА МЫСЛЕННЫХ ОБРАЗОВ НА ОСНОВЕ ЭЭГ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

С.М. Гончаров

В статье рассматривается схема разработки языка мысленных образов на основе ЭЭГ с использованием структуры нейросетевого преобразователя из ГОСТ 52633.5, описаны результаты предварительных исследований, подтверждающие высокий уровень распознавания ЭЭГ при воспроизведении определенных мысленных образов.

Ключевые слова: язык мысленных образов, ЭЭГ, высоконадежная биометрическая идентификация, интерфейс «мозг-компьютер», нейросетевой преобразователь.

ОПТИМИЗАЦИЯ АЛГОРИТМИЧЕСКОГО ПОДХОДА ОБНАРУЖЕНИЯ IMSI-ЛОВУШЕК В МОБИЛЬНОЙ СЕТИ СОТОВОЙ СВЯЗИ

А.Д. Уваров, Н.В. Кормильцев, Г.С. Корнилов

Недостаточная защищенность сети связи поколения 2G и обратная совместимость этого протокола с новыми стандартами 3G и 4G делают все мобильные сети уязвимыми для атак «Человек посередине» с использованием поддельных базовых станций («IMSI-ловушек»). Совсем недавно для большинства людей такое оборудование было довольно дорогостоящим и недоступным. Однако с падением цен на оборудование и появлением программного обеспечения с открытым исходным кодом можно построить IMSI-ловушку самостоятельно. Конфиденциальность пользователей еще никогда ранее не подвергалась такому уровню риска, как сегодня. Существующие системы обнаружения подобных ловушек основаны на программных приложениях, устанавливаемых на смартфоны или специализированные автономные системы, при этом главными недостатками данных систем являются высокая цена и ограниченный диапазон обнаружения. В данной статье будет предложен разработанный нами метод идентификации и обнаружения IMSI-ловушек, который использует существующую инфраструктуру GSM. Преимуществом данного метода является то, что он обеспечивает защиту всех пользователей от общего охвата сети оператора и экономит средства пользователей за счет отсутствия необходимости в приобретении дополнительного оборудования.

Ключевые слова: сотовая сеть, GSM, IMSI, MITM-атака, IMSI-ловушка, спуффинг, телекоммуникационная безопасность.

ОЦЕНКА КАЧЕСТВА И ОЧИСТКА ПЕРСОНАЛЬНЫХ ДАННЫХВ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

К.С. Сираева, Д.В. Катасёва, А.С. Катасёв

В статье рассматриваются вопросы оценки качества персональных данных в информационных системах организаций. С целью эффективной работы с персональными данными актуализируется необходимость их очистки. Для решения данной задачи разработана специальная методика. Произведен анализ ее эффективности на примере оценки качества и очистки дат рождения клиентов организации. Предложенная методика может быть использована в системах поддержки принятия решений для оценки качества, очистки персональных данных и приведения их к виду, пригодному для анализа.

Ключевые слова: оценка качества данных, очистка данных, персональные данные, моделирование.

ЗАЩИТА ИНФОРМАЦИИ В ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ ПРИ ПРЕДНАМЕРЕННЫХ МИКРОСЕКУНДНЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЯХ ПО СЕТИ ЭЛЕКТРОПИТАНИЯ

О.В. Чернов, Р.М. Гизатуллин, Э.А. Хузияхметова

В данной работе проводится моделирование защиты информации в вычислительной технике при воздействии преднамеренных микросекундных электромагнитных импульсов по сети электропитания. Проведен анализ путей проникновения электромагнитных импульсов к элементам вычислительной технике. Приведены результаты моделирования функционирования элементов вычислительной техники при воздействии преднамеренных микросекундных электромагнитных импульсов по сети электропитания.

Ключевые слова: защита информации, вычислительная техника, микросекундный электромагнитный импульс, сеть электропитания, моделирование.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОПЫТНО-КОНСТРУКТОРСКОМ БЮРО

К.С. Сираева, Д.В. Катасёва, А.С. Катасёв

В статье рассматриваются вопросы организации защиты персональных данных в опытно-конструкторском бюро. Анализируются общие требования по защите персональных данных. Приводится перечень и характеристика актуальных угроз безопасности персональных данных в организации. Определяется исходный уровень защищенности информационной системы персональных данных. Предлагаются технические и организационные меры по нейтрализации актуальных угроз. Указывается на необходимость совершенствования системы защиты персональных данных в опытно-конструкторском бюро как в обеспечении внешней защиты персональных данных сотрудников, так и при их хранении и обработке. Предлагаются конкретные меры для повышения эффективности организации защиты персональных данных.

Ключевые слова: персональные данные, защита информации, модель нарушителя, опытно-конструкторское бюро.

НЕЙРОСЕТЕВАЯ МОДЕЛЬ ДЛЯ ПРОГНОЗИРОВАНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

М.В. Дагаева, Д.В. Катасёва, А.С. Катасёв

В работе описывается технология применения нейронных сетей для решения задачи прогнозирования инцидентов информационной безопасности предприятия. Предлагается структура, производится обучение нейронной сети, оценивается ее адекватность и прогнозирующая способность. Показывается возможность эффективного использования нейросетевой модели в составе интеллектуальной системы прогнозирования.

Ключевые слова: нейронная сеть, временный ряд, прогнозирование, информационная безопасность, инцидент.

НЕСТРУКТУРИРОВАННАЯ ТЕКСТОВАЯ ИНФОРМАЦИЯ КАК ПОТЕНЦИАЛЬНЫЙ ИСТОЧНИК ИЗВЛЕЧЕНИЯ ЗНАНИЙ

К.С. Самолетова

В статье описывается проблема анализа массивов неструктурированной текстовой информации. Сравниваются понятия структурированных и неструктурированных текстов. Приводится некоторая классификация методов автоматического анализа текстовых документов. Рассматриваются сообщения из групп социальной сети Вконтакте в качестве источника получения новых знаний о заданном объекте.

Ключевые слова: большие данные, BIGDATA, инжиниринг знаний, DATA-MINING, неструктурированная информация, социальные сети.

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ ПОБОЧНОЙ КОНДУКТИВНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ ОТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЧЕРЕЗ СЕТЬ ЭЛЕКТРОПИТАНИЯ

Р.М. Гизатуллин, З.М. Гизатуллин, Э.С. Константинов

Наряду с программными методами защиты информации, повышенный интерес представляют методы физической защиты информации, связанные с побочными электромагнитными излучениями и кондуктивным наводками. Вероятным путем побочной кондуктивной передачи информации является кабель монитора - кабель электропитания

вычислительной техники. Разработан стенд и проводятся экспериментальные исследования побочной кондуктивной передачи информации от вычислительной техники через сеть электропитания. Приведены результаты измерения и проведено их сравнение с результатами моделирования.

Ключевые слова: защита информации, вычислительная техника, побочная кондуктивная передачи информации, сеть электропитания, эксперимент.

АУГМЕНТАЦИЯ ДАННЫХ И ПОСТРОЕНИЕ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ РАСПОЗНАВАНИЯ РУКОПИСНЫХ СИМВОЛОВ В СИСТЕМАХ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

М.В. Дагаева, Д.В. Катасёва, А.С. Катасёв

В данной статье рассматриваются вопросы построения систем биометрической аутентификации на основе нейросетевой модели распознавания рукописных символов. Подготовка исходных данных производилась с использованием метода аугментации. Для построения нейросетевых моделей использовались исходные и аугментированные данные. Для оценки точности моделей сформирована тестовая выборка, состоящая из обычных и искаженных образов десятичных цифр, отсутствующих в обучающих выборках. Точность исходной модели составила 87%, а точность аугментированной - 95%. Дополнительные расчеты показали снижение ошибок I рода в аугментированной модели по сравнению с исходной моделью на 3%, а число ошибок II рода - на 5%. Расчет общей ошибки моделей на основе метода трехблочной перекрестной проверки показал ее снижение на 0,14 за счет аугментации. Таким образом, аугментированная нейросетевая модель является эффективным инструментом распознавания рукописных символов в системах биометрической аутентификации.

Ключевые слова: нейронная сеть, аугментация, распознавание рукописных символов, биометрическая аутентификация.

ПОДХОД К ПРОЕКТИРОВАНИЮ И ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ ПО КОНТРОЛЮ ЗА СОБЛЮДЕНИЕМ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОТРУДНИКАМИ КОМПАНИИ

М.А. Бура, Ю.В. Гольчевский

Статья посвящена вопросам, связанным с исследованием подхода к проектированию и проведению мероприятий по контролю за соблюдением сотрудниками компании правил информационной безопасности.

Ключевые слова: социальная инженерия, информационная безопасность, контроль за соблюдением правил, фишинг, обучение персонала.

ЗАЩИТА ИНФОРМАЦИИ В ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ ПРИ ПРЕДНАМЕРЕННЫХ НАНОСЕКУНДНЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЯХ ПО СЕТИ ЭЛЕКТРОПИТАНИЯ

О.В. Чернов, Р.М. Гизатуллин, Э.А. Хузияхметова

Приведены результаты моделирования функционирования вычислительной техники при воздействии преднамеренных наносекундных электромагнитных импульсов по сети электропитания. Рассмотрены потенциальные параметры наносекундных электромагнитных импульсов. Разработаны количественные критерии оценки защиты информации в вычислительной технике при наносекундных электромагнитных воздействиях.

Ключевые слова: защита информации, вычислительная техника, наносекундный электромагнитный импульс, сеть электропитания, моделирование.

РОССИЙСКИЕ И ЗАРУБЕЖНЫЕ РАЗРАБОТКИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.Р. Оленева, Д.С. Семяшкина

В статье исследуются технические характеристики программно-аппаратных разработок отечественного и зарубежного происхождения в области обеспечения информационной безопасности.

Ключевые слова: средства защиты информации, DLP-системы, инциденты информационной безопасности.

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ О РАСПРЕДЕЛЕНИИ ЗАДАНИЙ ПО ВЕДЕНИЮ РЕЕСТРА ОПЕРАТОРОВ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕДИНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ РОСКОМНАДЗОРА

С.С. Кильдеева, Н.Г. Талипов, А.С. Катасёв, Д.В. Катасёва

В статье рассматривается задача распределения заданий по ведению реестра операторов персональных данных в единой информационной системе Роскомнадзора. Для ее решения предлагается использовать нечетко-продукционную модель. На основе модели разработан программный комплекс, выступающий в роли системы поддержки принятия решений для человека, ответственного за распределение заданий по исполнителям. Представлена схема обработки и распределения заданий с использованием программного комплекса. Приведены результаты его внедрения и практического использования.

Ключевые слова: реестр операторов персональных данных, система электронного документооборота, распределение заданий, поддержка принятия решений, нечетко-продукционная модель.

МОДЕЛИРОВАНИЕ ПОБОЧНОЙ КОНДУКТИВНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ ОТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЧЕРЕЗ СЕТЬ ЭЛЕКТРОПИТАНИЯ

Р.М. Гизатуллин, З.М. Гизатуллин, А.О. Архипов

Один из аспектов задачи информационной безопасности вычислительной техники связан с побочной кондуктивной передачей информации при ее обработке или передаче. Вероятным путем побочной кондуктивной передачи информации является кабель монитора - кабель электропитания вычислительной техники - система электропитания здания. В работе проводится моделирование побочной кондуктивной передачи информации от вычислительной техники через сеть электропитания. Приведены результаты моделирования побочных кондуктивных информационных сигналов в кабеле электропитания.

Ключевые слова: защита информации, вычислительная техника, побочная кондуктивная передача информации, сеть электропитания, моделирование.

РАСПОЗНАВАНИЕ ИЗОБРАЖЕНИЙ ЧЕЛОВЕЧЕСКОГО ЛИЦА НА ОСНОВЕ НЕЙРОСЕТЕВОЙ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ

М.В. Дагаева, Д.В. Катасёва, А.С. Катасёв

В данной работе проводится анализ методов построения систем идентификации и аутентификации личности по биометрии лица. Также анализируются существующие подходы к распознаванию образов. Разрабатывается нейросетевая биометрическая система распознавания личности по биометрии лица. Производится оценка ее эффективности на основе расчетов ошибок первого и второго рода, а также по методике кросс-валидации.

Ключевые слова: биометрическая система, идентификация, аутентификация, распознавание лиц, нейронная сеть, кросс-валидация, информационная безопасность.

РИСК-АНАЛИЗ И ПРОГНОЗИРОВАНИЕ АРЕАЛА РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В СООБЩЕСТВЕ "МДК"

В.В. Сафронова, К.В. Сибирко, Й. Воришек, В.И. Белоножкин, Л.В. Паринова

Статья направлена на изучение параметров деструктивного контента и ареала его распространения. Для этого были составлены микроареалы региональных интернет-пользователей, изучены тематики, представляющие наибольшую опасность при распространении ДК. Были предложены интегральные метрики контента, а также рассмотрены факторы, оказывающие влияние на его популярность.

Ключевые слова: деструктивный контент, риск, анализ, ареал распространения, метрики.

ОРГАНИЗАЦИЯ МОНИТОРИНГА ПОСТОВ СОЦИАЛЬНОЙ СЕТИ ВКОНТАКТЕ С ПОМОЩЬЮ ИНТЕРФЕЙСА VKAPI

А.Г. Остапенко, Е.Р. Нежельский, М.Н. Степанов, Е. Ружицкий, А.В. Заряев

В работе рассматривается процесс организации мониторинга деструктивного контента, циркулирующего в социальной сети Вконтакте. Измерение его параметров: ареала распространения, периода активности. Расчет вовлеченности пользователей в деструктивный контент. Расчет риска заражения пользователей.

Ключевые слова: мониторинг, ВКонтакте, VKAPI, измерение параметров, метрика, паблик, деструктивный контент, риск заражения.

РИСК-АНАЛИЗ ЯВЛЕНИЙ КИБЕРБУЛЛИНГА В СОБЫТИЙНЫХ ГРУППАХ СОЦИАЛЬНОЙ СЕТИ ВКОНТАКТЕ

В.С. Струков, Ю. Штефанович, Л.Г. Попова

В работе рассматривается феномен кибербуллинга в различных событийных группах социальной сети Вконтакте. Определяются ключевые особенности такого контента, участники, а также способы борьбы с ним.

Ключевые слова: кибербуллинг, травля, социальные сети, жертва кибербуллинга.