УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ СЛОЖНОЙ СЕТИ НА ОСНОВЕ МЕТОДА СТОХАСТИЧЕСКОГО ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ (ЧАСТЬ 1)

А.О. Калашников, Е.В. Аникина

В работе рассматривается подход к управлению информационными рисками сложной сети на основе метода стохастического имитационного моделирования.

Ключевые слова: критическая информационная инфраструктура, сложная сеть, управление, информационная безопасность, информационный риск, стохастическое имитационное моделирование.

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ СЛОЖНОЙ СЕТИ НА ОСНОВЕ МЕТОДА СТОХАСТИЧЕСКОГО ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ (ЧАСТЬ 2)

А.О. Калашников, Е.В. Аникина

В работе рассматривается подход к управлению информационными рисками сложной сети на основе метода стохастического имитационного моделирования.

Ключевые слова: критическая информационная инфраструктура, сложная сеть, управление, информационная безопасность, информационный риск, стохастическое имитационное моделирование.

ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ АДДИТИВНОЙ РОЛЕВОЙ МОДЕЛИ КОНТРОЛЯ ЗАЩИЩЕННОСТИ СИСТЕМ

А.О. Калашников, А.Ю. Максимовский

В статье для широкого класса информационных систем предложена аддитивная модель контроля защищенности, предполагающая совместное применение подсистемы внутреннего контроля системы и внешнего аудита. На основании указанной модели разработаны рекомендации по выбору параметров полсистемы внутреннего контроля системы и внешнего, аудита, а также оптимизации работ по поддержанию безопасного функционирования системы.

Ключевые слова: оценка защищенности, управление безопасностью, аудит безопасности, аддитивная модель.

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ СООТНОШЕНИЙ В АВТОМАТАХ ДЛЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ ОБЪЕКТОВ

А.О. Калашников, А.Ю. Максимовский

В работе рассмотрена модель мониторинга информационной безопасности объектов, сетевой инфраструктуры, основанная на контроле алгебраических и комбинаторных соотношений входных и выходных последовательностей указанных объектов.

Ключевые слов: критическая информационная инфраструктура, управление информационной безопасностью, комплексная оценка, кластерный анализ.

ИНСТРУМЕНТАРИЙ ГРАФОВЫХ БАЗ ДАННЫХ ДЛЯ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

П.Ю. Филяк, С.В. Королев, Н.В. Тебеньков

Рассматривается применение графовых баз данных (ГБД) для решения залач обеспечения информационной безопасности организации как комплексной проблемы, предусматривающей системный подход реализации целого ряда тесно взаимосвязанных задач. Решение данных задач является проблемой не тривиальной, поскольку организация является системой, обеспечение информационной безопасности также является системой с большим количеством подсистем и подзадач, которые не могут быть эффективно решены традиционными методами, поскольку по существу представляют собой сложные системы.

Ключевые слова: данные, информация, информационная безопасность, реляционные базы данных, стандарты, среда визуализации, графовые базы данных.

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В IP-СЕТИ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ АДАПТИВНО-РЕЗОНАНСНОЙ ТЕОРИИ С ИЕРАРХИЧЕСКОЙ СТРУКТУРОЙ ПАМЯТИ

Д.Г. Буханов, В.М. Поляков

Разработана структура системы обнаружений вторжений на основе интеллектуальных методов анализа. Предложена модифицированная структура АРТ-2 сети с многоуровневой памятью, архитектура которой позволяет значительно уменьшить время определения состояния компьютерной сети. Разработаны алгоритмы работы классификатора в параллельном режиме работы. На основе методики DigitalSecurity проведена оценка рисков функционирования информационной системы до и после внедрения разработанной системы обнаружений вторжений. Выполнена апробация системы на данных, представленных в выборке KDD.

Ключевые слова: система обнаружения вторжений, искусственные нейронные сети, адаптивно-резонансная теория.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ИНТЕРНЕТА ВЕЩЕЙ

П.Ю. Филяк, А.А. Изьюров, А.Л. Максимов, И.А. Тырин

Интенсивное развитие информационных и иитернет технологий создает новые способы взаимодействия во всех сферах. Одним из наиболее быстро развивающихся направлений информатизации - интернет вещей.

Ключевые слова: информация, информационная безопасность, интернет, иитернет вещей, цифровая экономика, уязвимость, угроза, риск.

МОДЕЛИРОВАНИЕ МЕТОДА МНОЖЕСТВЕННОГО ДОСТУПА С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

А.В. Яковлев, Д.А. Шибков, У.А. Савилова, М.А. Ивановский

В данной статье рассматривается технология метола множественного доступа с кодовым разделением каналов, разработка модели, реализующей данный метод, в среде MATEAB Simulink и проверка работоспособности и устойчивости к помехам созданной модели.

Ключевые слова: моделирование, множественный доступ с кодовым разделением каналов, функции Уолша, коды Голда.

ПРИМЕНЕНИЕ ГРАФОВОЙ БАЗЫ ДАННЫХ NTO4J ДЛЯ ОПТИМИЗАЦИИ ОБУЧЕНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

П.Ю. Филяк, С.В. Королев, Н.В. Тебеньков

Рассматривается подход к решению задачи оптимизации обучения по специальности и направлениям подготовки в области информационной безопасности, для чего в качестве варианта решения данной задачи, безусловно относящейся к области больших данных (Big Data), предложено применение информационно-аналитических систем, каковыми являются графовые базы данных. В качестве конкретного инструмента выбран Neo 4 j, на примере использования

которого становятся явно очевидными преимущества визуализации информации - современной методологии работы с большими информационными потоками.

Ключевые слова: данные, информация, информационная безопасность, большие данные (Big Data), цифровая экономика, федеральные государственные образовательные стандарты, учебный план, графовые базы данных.

ПОСТРОЕНИЕ НЕПРЕРЫВНЫХ ЗАКОНОВ РАСПРЕДЕЛЕНИЯ ДЛЯ ОЦЕНКИ РИСКОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Ю.Ю. Громов, Ю.В. Минин, В.Е. Дидрих, Н.Г. Шахов, С.А. Копылов

Для осуществления моделирования информационных систем и проведения экспериментов, связанных с оценкой рисков, необходимо рассматривать наборы случайных величии, распределенных по законам, получившим наиболее широкое распространение. При этом в работе наибольшее внимание уделяется законам распределения непрерывных случайных величин, обладающих максимальной энтропией. Для основных законов распределения, рассматриваемых в работе, получены выражения, обеспечивающие максимальное значение энтропии. Показано, что величины энтропии существенно зависит от типов используемых моментов, построенных на основе рассмотрения соответствующих законов распределения.

Ключевые слова: информационная система, риск, вероятность, закон распределения, энтропия.

ПРИМЕНЕНИЕ ГРАФОВОЙ БАЗЫ ДАННЫХ NEO4J ДЛЯ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, С.В. Королев, Н.В. Тебеньков

Рассматривается подход к решению задач обеспечения информационной безопасности, когда в качестве инструмента применяются информационно-аналитические системы, каковыми являются графовые базы данных. Графовые базы данных, с другой стороны, - инструмент работы с большими данными Big Data и получения из них знаний на основе Data Mining - интеллектуального анализа данных. В качестве конкретного инструмента работы с Big Data выбран Neo 4 j, на примере использования которого становятся явно очевидными преимущества визуализации информации - современной методологии работы с большими информационными потоками.

Ключевые слова: данные, информация, информационная безопасность, большие данные (Big Data), стандарты, интеллектуальный анализ данных (Data Mining), среда визуализации, графовые базы данных, информационно - аналитические системы (ИАС).

СРАВНЕНИЕ СПОСОБОВ РАСПРОСТРАНЕНИЯ СКРЫТЫХ МАЙНЕРОВ

А.В. Яковлев, М.В. Моисеева, Д.А. Яковлева, А.П. Рыжков

В статье представлен анализ различных способов распространения скрытых майнеров, а также способы зашиты от несанкционированных действий злоумышленника при реализации данной угрозы.

Ключевые слова: криптовалюта, скрытый майнинг, ботнет, преобразование трафика.

ГРАФОВАЯ СРЕДА GEPHI В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, Н.В. Тебеньков, С.В. Королев

Для решения задач информационной безопасности полезно, а иногда и необходимо, анализировать большие объемы данных. А при любом анализе отлично помогают средства визуализации. Gephi является очень мощным средством визуализации различных данных, который подойдет как новичку, так и опытному пользователю. Gephi - это дополнительный

инструмент для анализа, так как визуальное представление информации и работа с ним, помогает в решении задач.

Ключевые слова: Gephi, визуализация, граф. данные, информация, информационная безопасность, утечка.

ПРОЦЕДУРА ОПРЕДЕЛЕНИЯ КРИТИЧЕСКИХ ЭЛЕМЕНТОВ СЕТЕВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Р.А. Долбин, Ю.В. Минин, Г.Н. Нурутдинов, А.В. Высоцкий

В данной работе рассматривается вопрос оценки эффективности функционирования сетевой информационной системы. Представлен подход, позволяющий выявлять элементы сетевых информационных систем, которые являются критичными для сохранения требуемого уровня эффективности функционирования.

Ключевые слова: сетевая информационная система, эффективность функционирования, надёжность.

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, Н.В. Тебеньков, С.В. Королев

Информационные технологии в последние несколько лет стремительно развиваются. Достичь повышения уровня процедуры управления, тем самым улучшив качество администрирования в различных организациях, позволяют информационно – аналитические системы (ИАС). С их применением аналитик использует различные инструменты анализа, что позволяет решать задачи анализа и прогнозирования и принимать более объективные решения.

Ключевые слова: анализ, данные, информационная безопасность, информационно - аналитические системы, информация, среда визуализации.

ИССЛЕДОВАНИЕ ПОДХОДОВ К СОЗДАНИЮ ИНФОРМАЦИОННЫХ МОДЕЛЕЙ ДЛЯ СБОРА И ОБРАБОТКИ ДАННЫХ СОЦИАЛЬНЫХ СЕТЕЙ

В.Т. Ерёменко, М.А. Сазонов, С.В. Шекшуев

В статье анализируются существующие информационные модели данных с целью их использования для хранения и обработки данных из социальных сетей. Обосновывается актуальность исследования социальных сетей. Приводится сравнительная характеристика существующих информационных моделей, а именно иерархической, документной, реляционной и графовой. Раскрыто содержание каждой модели, се преимущества и нелостатки в задачах анализа данных из социальных сетей. Обосновывается превосходство использования графовой модели данных в указанном случае. Эффективность использования графовой модели данных подтверждена проведенным экспериментом. Исследование проводилось с использованием графовой СУБД Neo4j и языка запросов Cypher.

Ключевые слова: социальная сеть; модели данных; иерархическая модель данных; документная модель данных; реляционная модель данных; СУБД: Neo4j; Cypher.

ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ IOT-СЕТИ НА ПРИМЕРЕ РЕАЛИЗАЦИИ ТЕХНОЛОГИИ УМНЫЙ ДОМ

С.А. Ермаков, А.А. Болгов, А.Н. Мокроусов

Предлагается методика численного расчета показателя эффективности защиты сети IoT для различных вариантов конфигурации протоколов взаимодействия элементов системы «Умный дом», а также даны практические рекомендации по увеличению показателя защиты сети, основанные на конкретном примере.

Ключевые слова: сеть IoT, технология умный дом, нечеткие множества, риск, беспроводные сети, защита, эффективность.