МЕТОДИКА ОЦЕНКИ ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ

А.О. Калашников, К.А. Бугайский

В работе предложена методика оценки возможности реализации информационных угроз нарушителем на основе расчета расхождения между текущими и эталонными параметрами. Текущие и эталонные параметры определяются на основе характеристик CVE базы данных NVD NIST, а также иерархии CWE и CAPEC баз данных MITRE. Предложен алгоритм отбора уязвимостей, обеспечивающий проактивный подход к определению угроз информационной системы. В рамках методики разработана модель информационной системы как набора элементов, характеризуемых набором угроз и распределением прав доступа. Предложены механизмы нормализации параметров в условиях неравномерности выборок для отдельных элементов информационной системы. Показана возможность применения результатов для оценки угроз и потенциала нарушителя, а также для определения актуальных угроз безопасности информации.

Ключевые слова: защита информации, методика оценки, оценка нарушителя, оценка угроз, оценка риска.

ПРОБЛЕМЫ СБОРА, ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ – УЧАСТНИКОВ ОНЛАЙН КОНКУРСОВ И ТЕСТИРОВАНИЯ

П.Ю. Пушкин, Е.В. Никульчев, В.П. Лось

Целью работы является анализ соблюдения требований законодательства, этических норм при обработке персональных данных организаторами онлайн мероприятий для школьников и студентов. Предложены рекомендации по обработке персональных данных при проведении онлайн тестирований и олимпиад. Новизна работы заключается в определении отличительных (отраслевых) особенностей обработки персональных данных при организации и проведении онлайн тестирований, конкурсов, олимпиад, в разработке методики поэтапного сбора персональных данных с определением необходимого их объема на каждом этапе. Результаты: определены основные проблемные вопросы обработки персональных данных обучающихся, участвующих в онлайн конкурсах, олимпиадах, тестированиях; произведена их классификация на нормативные, этические (связанные с культурой сбора и обработки персональных данных), организационные и технические. Определены отраслевые отличительные особенности обработки персональных данных участников онлайн мероприятий. Разработаны рекомендации по проведению онлайн олимпиад и конкурсов, повышающие уровень защищенности персональных данных обучающихся, в том числе методика поэтапного увеличения объема собираемых персональных данных участника. Анализ интернет-ресурсов онлайн мероприятий показал отсутствие единого отраслевого подхода к организации и проведению работ по защите персональных данных участников таких мероприятий, который предложено разработать. Практическая значимость: обозначенные проблемные вопросы организации онлайн мероприятий с использованием персональных данных обучающихся и разработанные предложения по повышению их уровня информационной безопасности могут использоваться при составлении отраслевых (образовательных) рекомендаций по защите персональных данных участников онлайн олимпиад, иных подобных мероприятий.

Ключевые слова: цифровое общество, персональные данные, обезличенные данные, защита информации, онлайн тестирование, олимпиады школьников.

МОДЕЛИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ СЛОЖНЫХ СИСТЕМ

А.О. Калашников, Е.В. Аникина

В работе рассматривается базовая модель управления информационными рисками сложных систем, в рамках которой два субъекта произвольной природы, называемые атакующий (*attacker*) и защитник (*defender*), путем распределения имеющегося в их распоряжении ресурса между элементами сложной системы, осуществляют воздействие на состояние элементов системы и системы в целом. Для оценки состояния элементов системы используются функции локального риска, удовлетворяющие некоторым заданным требованиям, а для оценки состояния системы в целом – функция интегрального риска. Поскольку субъекты (атакующий и защитник), имеют, вообще говоря, несовпадающие интересы относительно финального состояния сложной системы возникает теоретико-игровое конфликтное взаимодействие между ними, свойства которого могут уточняться в рамках конкретизации и обобщения базовой модели. Некоторые примеры подобного рода конкретизаций и обобщений базовой модели, в том числе, модели управления информационными рисками в условиях неопределенности, в условиях взаимного влияния элементов системы друг на друга, в условиях информационного противоборства и ряд других, также рассмотрены в настоящей работе.

Ключевые слова: сложная система, управление риском, информационный риск, защитник, атакующий.

КАРТОГРАФИЧЕСКИЙ ПОДХОД ИССЛЕДОВАНИЯ ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В СООБЩЕСТВАХ ЕДИНОЙ ТЕМАТИКИ СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ»

А.Л. Сердечный, Р.В. Марков, И.В. Герасимов, А.Е. Гуслянников, И.А. Боков

В данной работе был предложен подход к исследованию динамики распространения деструктивного контента при помощи визуального метода представления пространства социальных сетей и протекающих в них процессов в виде карт, подобных географическим картам. Подход представляет собой итеративное выполнение следующих действий: подготовку исходных данных, разработку интерактивной карты анализируемого пространства сообществ социальной сети, расчёт метрик, визуализацию процесса распространения деструктивного контента, интерактивного анализа построенных карт. Подход продемонстрирован на примере анализа распространения деструктивного контента в сообществах социальной сети «ВКонтакте», связанных между собой единой тематикой и наличием общих участников. Реализация подхода осуществлялась при помощи разработанного программного средства, включающего: подсистемы сбора, хранения и визуализации данных. В рамка реализации подхода предложен показатель расчёта риска распространения деструктивного контента на основании размера площади области активности пользователей.

Ключевые слова: картографический подход, киберпространство, социальные сети, визуализация, площади области активности пользователей, риск.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ BLOCKCHAIN ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ЭКОНОМИКЕ

П.Ю. Филяк, А.О. Басенко, А.В. Лукин

Рассматривается подход к обеспечению информационной безопасности путем применения концепции технологий BlockChain. Данный подход не является традиционным по отношению к сфере обеспечения информационной безопасности, однако в условиях развития цифровой экономики, достаточно давно и широко использующей возможности концепции BlockChain, эффективность использования данного подходя становится вполне очевидной. Информационная

безопасность, являясь системой, механизмом и процессом, по сути такая же технологическая цепочка, как и любой бизнес-процесс. Несовершенство технологического процесса, реализуемого в рамках традиционного управления приводит к большим потерям времени, финансовым издержкам. Эти проблемы можно решить при реализации сети распределенных реестров, в которой данные о транзакциях строятся в виде цепи блоков, связанных между собой и хранящих информацию о совершённых транзакциях. Для реализации подхода использована платформа с открытым исходным кодом Ethereum. Программная реализация проведена с помощью интерфейса MyCrypto.

Ключевые слова: безопасность, структуры – централизованные, децентрализованные, распределенные, технологическая цепочка, BlockChain, смарт – контракт, электронный кошелек.

МОДЕЛЬ ВЫЯВЛЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫЕ СЕТИ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ АДАПТИВНО-РЕЗОНАНСНОЙ ТЕОРИИ

Д.Г. Буханов

В работе был проведен анализ существующих моделей и методов обнаружений вторжений в компьютерные сети. Выявлены основные недостатки существующих моделей обнаружения вторжений. Выявлено, что наиболее перспективными являются модели использующие искусственные нейронные сети. Предложена модель обнаружения вторжений, в состав которой входит классификатор состояния компьютерной сети на основе адаптивно-резонансной теории с иерархической структурой памяти. Использование такой модели позволяет придать свойства адаптивности и расширяемости системам обнаружения вторжений. Помимо этого, предложенная модель позволяет на основе дерева памяти классификатора выполнять, как отложенный анализ, так и анализ в режиме реального времени, возникающих новых состояний в компьютерной сети. Проведены экспериментальные исследования времени обучения предложенной модели. В работе продемонстрированы основные преимущества предложенной модели и визуально представлен процесс дообучения классификатора.

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

«ИНФОДЕМИЯ» И СОЦИАЛЬНЫЕ СЕТИ: ИНДУЦИРОВАННЫЕ РИСКИ И ШАНСЫ

А.Г. Остапенко, Е.А. Шварцкопф, А.А. Остапенко, Т.Ю. Мирошниченко, С.Д. Трубицын, Н.М. Лантюхов, А.Н. Бартенев

Работа посвящена анализу уникального явления, получившего название «инфодемия». Порожденное пандемией коронавируса, это явление охватило миллиарды пользователей сети Интернет и прежде всего её социальных сетей. В этой связи в работе, исходя из результатов контент-мониторинга, исследуется тематическое пространство инфодемии, которое беспрецедентно возбудило социум. Анализ показал появление целого спектра угроз. Индуцированные при этом риски показали их встроенность (через положительную обратную связь) в угрозу потери управляемости социумом посредством глобальных информационных возмущений, обусловленных огромным психологическим влиянием социальных сетей на общественное мнение широких масс населения планеты. При этом рассматриваются и шансы глубокой модернизации архитектуры мироустройства.

Ключевые слова: пандемия, инфодемия, угрозы, риски, шансы.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ СЕМАНТИЧЕСКИХ СЕТЕЙ

И.А. Земцов, О.Г. Иванова, Ю.В. Минин, С.В. Данилкин

В последнее время обширная исследовательская деятельность направлена соблюдение чистоты поисковой выдачи для информационной безопасности интеллектуальных систем. Однако, ключевая технология сети интернет эволюционирует в новую форму поиска в семантическом интернете. Перспективный подход к такому семантическому поиску в интернете основан на объединении стандартных поисковых машин в качестве основного вывода результатов семантического поиска. В этой статье рассматривается способ семантического поиска, объединяющий преимущества стандартных поисковых машин и алгоритмов семантического поиска.

Ключевые слова: семантика, аналитическая модель поиска, семантическая сеть, сбор данных, информационная безопасность, обнаружение знаний.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОСТРОЕНИЯ СОВМЕЩЕННОЙ МОДЕЛИ УГРОЗ И НАРУШИТЕЛЯ

М.Ю. Рытов, О.М. Голембиовская, Н.Е. Боровых, К.Е. Шинаков

Цель данного исследования - разработка автоматизированной системы построения совмещенной модели угроз и модели нарушителя по проекту методики 2015 года ФСТЭК. Автоматизированная система – система, функционирующая с персоналом путем применения комплекса средств автоматизации его деятельности. В исследовании обоснованы причины для разработки автоматизированной системы. Выстроен алгоритм работы автоматизированной системы. Рассмотрена модель работы системы на примере организации, описаны все этапы работы (определение уровня проектной защищенности/защищенности, потенциала нарушителя, степени ущерба, актуальности угрозы безопасности, занесение информации в модель угроз). Данная работа включает в себя алгоритм работы автоматизированной системы, таблицы и формулы для определения показателей, используемых в системе. Полученная автоматизированная система представляет практическую ценность для автоматизации построения модели угроз и модели нарушителя по проекту методики 2015 года ФСТЭК с выводом на экран информации о возможности реализации угрозы и о ее актуальности.

Ключевые слова: информационная безопасность, модель угроз, модель нарушителя, автоматизированная система.

ИСПОЛЬЗОВАНИЕ СЕМАНТИЧЕСКОЙ СЕТИ ДЛЯ ВЫБОРА ЗНАНИЙ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

И.А. Земцов, О.Г. Иванова, Ю.В. Минин, С.В. Данилкин

С развитием технологий стабильность информационной безопасности интеллектуальных систем и механизм обнаружения знаний в семантической сети на основе ключевых слов недостаточны из-за извлечения большого количества нерелевантной информации. В статье предложена семантическая поисковая система, в которой решена эта проблема. Описан алгоритм обнаружения знаний в семантической сети на этапе выбора соответствующих предварительных знаний с использованием связанных открытых данных для интерпретации реляционных баз данных и неструктурированных данных для повышения информационной безопасности интеллектуальных систем, заключающийся в комбинировании подходов, которые выполняют согласование схемы и экземпляра в целостном виде. Результат исследования показал большую эффективность предложенной системы по сравнению с использующими подходы, в которых согласование схемы и экземпляра в целостном виде происходит изолированно.

Ключевые слова: семантика, алгоритм поиска, семантическая сеть, сбор данных, обнаружение знаний, информационная безопасность, интеллектуальный мультимодальный интерфейс.

ОПТИМАЛЬНОЕ РАСПРЕДЕЛЕНИЕ КАДРОВЫХ РЕСУРСОВ В МНОГОУРОВНЕВОЙ СИСТЕМЕ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ

В.А. Минаев

В статье показано, что основным трендом для государственных структур и крупных межотраслевых и отраслевых корпораций выступает построение Центров мониторинга информационной безопасности, ключевыми элементами которых являются SIEM-системы и SOC - Центры. Применительно к SOC - Центрам актуальна задача оптимального распределения кадровых ресурсов между линиями обслуживания сообщений об инцидентах информационной безопасности с учетом компетентности персонала. Эта задача решается в настоящей работе. В общем виде постановка задачи управления заключается в представлении функционирования SOC - Центра в терминах “вход – ресурсы – выход” в виде новой математической модели. В предположении стационарности и независимости функционирования линий обслуживания строится целевая функция SOC – Центра в виде суммы их целевых функций. Основной идеей управления кадровыми ресурсами в этом случае является стремление достичь SOC-Центром максимального значения своей системной цели, т.е. его общей целевой функции при организации борьбы с компьютерными атаками. Задача решалась методом множителей Лагранжа. Получены выражения для оптимального распределения кадровых ресурсов по линиям обслуживания SOC-Центра, которое приводит к достижению максимального обслуживания потока сообщений о компьютерных атаках. Кроме того, оценены значения потоков сообщений об атаках для каждого уровня по трем категориям: опасные для компьютерной системы, не представляющие для нее угроз, переданные на более компетентный уровень принятия решений. Сделан вывод о полезности модели для перехода от стационарных потоков к их динамическим изменениям, включая возникновение различных критических ситуаций в компьютерной системе, в ресурсном обеспечении SOC-Центра.

Ключевые слова: информационная безопасность, мониторинг, SOC-центр, компьютерная атака, принятие решений, оптимальное распределение кадровых ресурсов.

АВТОМАТИЗАЦИЯ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИИ И КОНТРОЛЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

П.Ю. Филяк, В.В. Растворов

В статье рассматриваются подходы, позволяющие автоматизировать управление контроля доступа к информации согласно мандатной модели доступа и реализация контроля целостности. Ограничение доступа к свойствам информации достигается за счет политик управления доступом, с помощью которых можно реализовать защиту информации разного уровня доступа. В статье рассмотрены алгоритмы и программная реализация присвоения прав доступа. Предложено комплексное использование механизмов реализации политик информационной безопасности организаций, основанных на принятых в организациях правил разграничения доступа, средств и систем разграничения доступа к информации.

Ключевые слова: Политика доступов, права доступов, автоматизированная система, модель, безопасность, мандатная политика управления доступом, система защиты, защищенность.

«ИНФОДЕМИЯ» И СОЦИАЛЬНЫЕ СЕТИ: МОДЕЛИ ЭПИДЕМИЧЕСКОГО ПРОЦЕССА

А.Г. Остапенко, Е.А. Шварцкопф, А.А. Остапенко, Д.А. Нархов, П.Д. Федоров, Р.В. Сорокин

Работа посвящена моделированию инфодемии. В этой связи предполагается графовая модель инфицирования пользователя сети вирусным контентом, учитывающая сетевую и индивидуальную специфику пользователя в восприятии данного контента. Кроме того, в работе представлена детализация алгоритмики пошагового развития инфодемии через распространителей психологического вируса с оценкой мощностей множеств пользователей с различным статусом (незараженные, иммунизированные, распространяющие и недееспособные в сети), включая этапы первичного, вторичного и последующего инфицирования атакуемой сети. Наряду с вышеизложенным в работе предложены аналитические оценки параметров инфодемии (рисков неблагоприятного и шансов позитивного развития процесса, сетевой эпистойкости на каждом шаге мониторинга).

Ключевые слова: инфодемия, контент, графовая модель, риск, шанс, эпистойкость.

ИНСТРУМЕНТАРИЙ ДЛЯ ИССЛЕДОВАНИЯ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ В УСЛОВИЯХ РАСПРОСТРАНЕНИЯ ВИРУСНОГО КОНТЕНТА: ТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВРЕДОНОСОВ

Е.Ю. Чапурин, Н.И. Свиридов, Е.А. Шварцкопф, С.С. Тихонова, Д.С. Хохлова, И.А. Боков, Т.Ю. Мирошниченко

В работе предложены методы повышения точности определения тематики вирусного контента за счет включение в рамки анализа помимо текста, количество которого в сети Интернет постоянно уменьшается, также различного вида изображений, содержащих вирусный контент. Также в статье рассматривается и решается задача построения корпуса биграмм для осуществления тематического моделирования в условиях ограниченности аппаратных ресурсов на основе не полностью структурированных данных. Помимо этого, описывается алгоритм построения архитектуры программного комплекса, который может быть интегрирован в существующую систему анализа интернет-пространства.

Ключевые слова: информационные сети, распределенные компьютерные системы, вирусный контент, тематическое моделирование.

МОДЕМЫ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ СВЯЗИ И УПРАВЛЕНИЯ: ЗАЩИТА ОТ АТАК ВНЕДРЕНИЯ ВРЕДОНОСНОГО КОДА НА ОСНОВЕ ЭКСПЕРТНОЙ ОЦЕНКИ СРЕДСТВ ЗАЩИТЫ МОДЕМА И РЕГУЛИРОВАНИЯ РИСКОВ

А.В. Гречишкин, Д.Н. Рахманин, А.В. Свиридов, И.А. Боков, Т.Ю. Мирошниченко

В статье предложен алгоритм проведения и проверки экспертного оценивания средств защиты от атак внедрения кода с последующим использованием результатов для оценки и регулирования рисков атак внедрения кода на модемы телекоммуникационных систем связи и управления. Проведен анализ внедрения кода как атаки на модем, анализируется использование сформулированных в банке данных угроз ФСТЭК России угроз внедрения кода в сценарных описаниях реальных атак. Описаны основные этапы алгоритма оценки и регулирования рисков, возможных на современный момент путей их решения. Получены численные оценки для комплексов защиты памяти модемов телекоммуникационных систем связи и управления. Полученные результаты показывают насколько защищена та или иная комбинация средств защиты памяти модемов телекоммуникационных систем связи и управления.

Ключевые слова: модем, система, управление, связь, атака, внедрение кода, алгоритм, оценка, моделирование, нечеткие множества.