О ВЫБОРЕ ПАРАМЕТРОВ АВТОМАТНЫХ МОДЕЛЕЙ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ ОБЪЕКТОВ (ЧАСТЬ 2)

А.Ю. Максимовский

В статье изучаются свойства сложных систем, представимых в виде сети автоматов, обладающих специальными свойствами. Данные свойства используются в интересах организации наблюдения за динамикой изменения (мониторинга) поведения состояния указанных систем в целях обеспечения надежного контроля функционирования. При этом в множество критериев контроля могут включаться результаты проверки соответствия троек входных последовательностей, последовательностей состояний и выходных последовательностей объектов контроля набору отношений, формируемых с использованием информации о свойствах рассматриваемых автоматных моделей сетевых объектов и, в частности, особенности функционирования указанных автоматных моделей. Предложены дальнейшие пути развития методов и средств выявления особенностей внешнего поведения автоматных моделей объектов контроля, способы построения и использования экспериментов с автоматами, а также отношений специального вида для автоматных моделей компонентов сложных систем и ассоциированных с ними комбинаторных объектов, определяемых на мультиграфах состояний соответствующих автоматов. Указаны общие подходы к применению автоматных моделей регистрового типа для мониторинга информационной безопасности сетевых объектов регистров сдвига или их обобщений, обладающие необходимыми свойствами. Получены новые результаты о возможностях и предложены новые подходы к выбору характеристик применения рассмотренных ранее автоматных моделей. Основное внимание уделено изучению групп автоматных моделей обобщенных недвоичных регистров сдвига и их обобщений, обладающих необходимыми свойствами. На основании этих результатов построены новые классы автоматных моделей параметров мониторинга информационной безопасности объектов сетевой инфраструктуры, которые включают не только основанные на контроле алгебраических и комбинаторных соотношений входных и выходных последовательностей указанных объектов, но и позволяют выявить потенциальные угрозы безопасности средствам контроля.

Ключевые слова: мониторинг безопасности функционирования сетевых объектов, критическая информационная инфраструктура, конечный автомат, группа автомата, регистр сдвига, диаметр графа.

СТАТИСТИЧЕСКИЕ ОСОБЕННОСТИ ДИНАМИКИ ИНФОРМАЦИОННЫХ ОБМЕНОВ В СОЦИАЛЬНЫХ СЕТЯХ

М.И. Купцов, В.А. Минаев

Для целей изучения динамики информационных обменов в социальных сетях и прогнозирования на этой основе реальных общественных акций предложена классификации групп пользователей сетей на четыре категории: маркетинговые, политические, блогерские, индивидуальные. Изучены эмпирические распределения различных статистических показателей активности названных категорий в сети «ВКонтакте» применительно к коротким (до 100 дней) и длинным (более 100 дней) промежуткам времени. Показано существование устойчивых нормальных, равномерных и экспоненциальных распределений исследованных статистических показателей и статистически устойчивых связей между ними, пригодных для обоснования динамики развития информационных обменов в социальных сетях и дающих возможность строить регрессионные модели для оценки количества участников различных общественных акций, включая протестные движения. Делается вывод, что следующий шаг в исследованиях данного направления должен быть связан с более глубоким изучением факторов, влияющих на распространение информации в социальных сетях. К ним относятся: дальнейшая дифференциация статистических исследований применительно к маркетинговым, политическим и блогерским сообществам; более детальное изучение устойчивости статистических зависимостей на длинных и коротких временных отрезках; сочетание статистического анализа структуры выделенных сообществ с имитационным моделированием динамики переходов между их группами с учетом латентных (ненаблюдаемых) состояний.

Ключевые слова: социальная сеть, распространение информации, моделирование, прогнозирование, статистические закономерности.

ТЕХНОЛОГИЯ ВЫЯВЛЕНИЯ СВЕДЕНИЙ ОБ УЯЗВИМОСТЯХ СТОРОННИХ КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

А.Л. Сердечный, И.В. Герасимов, О.Ю. Макаров, Ю.Г. Пастернак, Н.М. Тихомиров

В статье приведены результаты разработки технологии выявления сведений об уязвимостях сторонних компонентов программного обеспечения (ПО), позволяющей своевременно обнаруживать проблемы безопасности, связанные с использованием заимствованных компонентов с открытым исходным кодом. Технология отличается процедурами оперативного обнаружения, ранжирования и подтверждения достоверности первоисточников сообщений о таких проблемах. Разработанная технология основана на проведении сбора и семантического анализа сведений об ошибках и средствах (алгоритмах) эксплуатации уязвимостей ПО, содержащихся в сообщениях, публикуемых на информационных ресурсах разработчиков ПО с открытым исходным кодом. Технология включает процедуру подтверждения сведений о наиболее опасных уязвимостях с последующей оценкой рисков для подтверждённых уязвимостей. В статье также приводятся результаты реализации предлагаемой технологии в виде средства сбора и интерактивного анализа сообщений о ошибках в ПО с открытым исходным кодом, размещаемым на платформах для совместной разработки GitHub и GitLab. Технология выявления сведений об уязвимостях сторонних компонентов позволяет повысить защищённость ПО, использующего в своём составе общедоступные компоненты с открытым исходным кодом.

Ключевые слова: безопасная разработка, выявление уязвимостей, стороннее программное обеспечение, программа с открытым исходным кодом, поисковая карта научных публикаций.

АУДИТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА – ОПЫТ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ

П.Ю. Филяк, А.Н. Ермолин, М.А. Корецкий

Искусственный интеллект (Artificial Intelligence – AI) в настоящее время это уже не просто модное название и словосочетание, а система мышления (когнитивная система), моделирующая работу головного мозга, мышления и принятия им целого спектра решений, в том числе и управленческих. Искусственный интеллект – реализуемая с помощью программно-аппаратного обеспечения и использующая разнообразный набор типов интерфейсов и их сочетаний, позволяющих осуществлять практически полноценную замену традиционно используемых человеческих мыслительных и управленческих функций для решения как теоретических, так и практических задач, начиная от простых, легко структурируемых задач и вплоть до задач, характеризующихся неопределенностью. В статье рассмотрены этапы последовательной реализации искусственного интеллекта. Приведен пример создания навыка для голосового ассистента на языке PHP.

Ключевые слова: информационная безопасность, логика, анализ, искусственный интеллект, большие данные, мышление, когнитивные процессы, навыки, машинное обучение, тренировка, модерация.

ДЕСТРУКТИВНОСТЬ КОНТЕНТА, ЕГО КЛАССИФИКАТОРЫ И СКАНЕРЫ ДЛЯ РИСК-АНАЛИЗА СОЦИАЛЬНЫХ СЕТЕЙ

Е.Ю. Чапурин, А.Е. Гуслянников, К.А. Разинкин, И.А. Батаронов

В статье рассмотрены вопросы анализа контента социальных сетей для выявления признаков деструктивности, используемых при программном сканировании. Сделан вывод о том, что методы семантического и морфологического анализа текста, а также анализ тональности текста индивидуально не дают необходимый результат. Поэтому необходимо анализировать текст при помощи нескольких методов анализа текста в совокупности. Также необходимо использовать N-граммы для анализа, так как этот метод позволяет находить необходимые слова с большей точностью. Для работы со сканерами были выбраны самые оптимальные методы работы с социальными сетями. В связи с тем, что в социальной сети «Одноклассники» есть ограничения с работой API, был выбран метод сканирования на основе библиотеки phpQuery.

Ключевые слова: социальная сеть, анализ, программы-сканеры, контент.

ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

П.Ю. Филяк, А.Н. Ермолин, М.А. Корецкий

В статье представлены подходы к решению проблем обеспечения информационной безопасности на основе использования искусственного интеллекта с позиций возможности реализации на практике вариантов воплощения программной и аппаратной частей потенциального функционала искусственного интеллекта в данной сфере. В статье рассмотрены вопросы обучения и интерфейса искусственного интеллекта с внешней средой. Обсуждается создание навыков голосового интерфейса для искусственного интеллекта. Представлен анализ категории «Искусственный интеллект» и приведена последовательность «подготовительных» действий, необходимых для практической реализации каких-либо управленческих функций человека, независимо от сферы применения, на основе искусственного интеллекта.

Ключевые слова: информационная безопасность, логика, искусственный интеллект, мышление, когнитивные процессы, навыки, машинное обучение, тренировка, модерация.

ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС ДЛЯ РИСК-АНАЛИЗА ДЕСКТРУКТИВНЫХ КОНТЕНТОВ СОЦИАЛЬНЫХ СЕТЕЙ: СТРУКТУРА, ВНЕШНИЙ ВИД И БАЗЫ ДАННЫХ

Е.Ю. Чапурин, А.Е. Гуслянников, Л.В. Паринова, В.Г. Юрасов, Ю.Г. Пастернак

В статье описан разрабатываемый программно-технический комплекс, представляющий собой веб-платформу с интегрированными программами-сканерами и анализатором текста. Приведен перечень языков программирования, с помощью которых был разработан программно-технический комплекс. Наряду с этим представлен внешний вид программно-технического комплекса для выявления и анализа деструктивного контента. Представлен внешний вид десктопной и мобильной версии программно-технического комплекса, примеры авторизации. Описан процесс регистрации на платформе для поиска деструктивного контента и проведения риск-анализа. Приведен перечень основных блоков, которые становятся доступные после авторизации в личном кабинете. Также рассмотрена система баз данных, ее внешний вид и описаны все поля используемых таблиц (Log_pass, Users, Login_base, Comments, Emotions_ok, get_users_likes, groupsdestructive, groupsdestructive_log, Queries) и их применение.

Ключевые слова: социальная сеть, анализ, программы-сканеры, данные.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ BLOCKCHAIN ДЛЯ РАЗРАБОТКИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

П.Ю. Филяк, М.К. Постников, С.Е. Федоров

В условиях развития информационного общества (Knowledgeable society – KS) информационные системы стали неотъемлемой частью любой организации, даже самой малой, независимо от реализуемых ими бизнес-процессов. Такие информационные системы принято называть корпоративными информационными системами (КИС), или Corporate Information System (CIS). Особые требования при разработке КИС предъявляются к обеспечению их информационной безопасности, что может быть реализовано путем разработки КИС в защищенном исполнении. Технологии blockchain являются очень перспективными не только при применении их в традиционных сферах – производстве, сервисе, на транспорте, но и для решения проблем безопасности и информационной, в частности. Анализу данной проблемы и подходам к ее решению и посвящена данная статья.

Ключевые слова: информационное общество, информационная система, корпоративная информационная система (КИС), информационная безопасность (ИБ), корпоративная информационная система в защищенном исполнении (КИС в ЗИ).

ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС РИСК-АНАЛИЗА ДЕСТРУКТИВНЫХ КОНТЕНТОВ СОЦИАЛЬНЫХ СЕТЕЙ: ОСНОВНЫЕ КОМПОНЕНТЫ И УЯЗВИМОСТИ

Е.Ю. Чапурин, А.Е. Гуслянников, Л.В. Паринова, В.Г. Юрасов, Ю.Г. Пастернак

В статье описана работа программ-сканеров. Для программы-сканера социальной сети «ВКонтакте» предложена методика работы с API данной сети, включая проверку на существование токена авторизации, а при его отсутствии описан метод получения токена и дальнейшее его применение. Для программы, работающей с социальной сетью «Одноклассники», описаны вспомогательные функции, основанные на библиотеке cURL, необходимые для получения DOM-страницы и ее хранения. Также изложена логика программы-сканера с последующим анализом функций библиотеки phpQuery. Описана работа программы-классификатора, включая подробное описание примененных методов библиотеки php-ml на основе метода опорных векторов. Проведен анализ комплекса на наличие уязвимостей.

Ключевые слова: социальная сеть, анализ, программы-сканеры, уязвимость, контент.

ПРАКТИКА РЕАЛИЗАЦИИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ НА ОСНОВЕ ТЕХНОЛОГИЙ BLOCKCHAIN

П.Ю. Филяк, М.К. Постников, С.Е. Федоров

В статье рассматривается практическая реализация варианта корпоративной информационной системы в защищенном исполнении (КИС в ЗИ/КИС ЗИ) на основе использования технологии блочейн (blockchain) вместе с «десктопным» (Desk Top) и соответствующими интерфейсами пользователя. Технологии Block Chain являются очень перспективными не только при применении их в традиционных сферах – производстве, сервисе, на транспорте, но и для решения проблем безопасности, в частности, информационной, что наглядно продемонстрировано опытом успешного применения криптовалют на протяжении последних десятилетий. Актуальность использования технологий Block Chain для создания корпоративной информационной системы в защищенном исполнении – отдельная тема, являющаяся «предтечи» непосредственной реализации на практике данной задачи.

Ключевые слова: корпоративная информационная система (КИС), информационная безопасность, защищенное исполнение, десктопное приложение, интерфейс, логи.

КАРТОГРАФИЧЕСКОЕ ИССЛЕДОВАНИЕ ДЕЯТЕЛЬНОСТИ КИБЕРПРЕСТУПНЫХ ГРУППИРОВОК В КОНТЕКСТЕ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ

Е.А. Москалева, Н.И. Баранников, Д.С. Каребин, И.Л. Батаронов, О.Ю. Макаров

Целью исследований является определение мер защиты от наиболее опасных киберпреступных группировок в ходе картографических исследований их деятельности в распределенных компьютерных системах. В работе продемонстрирован картографический подход к решению задачи выявления взаимосвязей киберпреступных группировок на примере построения и анализа карт связей группировок и используемых ими средств, а также технических приёмов. При помощи интерактивной карты выявляют киберпреступные группировки, которые проводят массовые атаки, и на основе этого разрабатывают меры защиты от средств, используемых во время атак. Результаты статьи полезны для повышения эффективности экспертного анализа, позволяющего быстрее находить взаимосвязи, установление которых было затруднено в силу отсутствия визуальной составляющей представления данных, так и для защиты информационных систем пользователей, которые могут стать жертвами массовых компьютерных атак.

Ключевые слова: картографический подход, киберпреступные группировки, APT-атаки, анализ, визуализация.

МОДЕМЫ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ СВЯЗИ И УПРАВЛЕНИЯ: ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИСПОЛНИТЕЛЬНОЙ ПРОГРАММЕ

А.В. Гречишкин, Д.Н. Рахманин, В.Ю. Пустовалов, О.Ю. Макаров, Н.И. Баранников, В.Г. Юрасов

В работе рассматривается проблема защиты от несанкционированного доступа к исполнительной программе модемов телекоммуникационных сетей связи и управления, а также предлагается порядок реализации программного средства защиты. Проводится анализ уязвимостей и угроз, характерных телекоммуникационным устройствам, спроектированным на базе микроконтроллеров общего назначения, а также рассматриваются возможности противодействия наиболее актуальным видам атак. Анализируются варианты применения криптографических примитивов для реализации средства защиты от несанкционированного доступа к исполнительной программе модемов телекоммуникационных сетей связи и управления и предлагается подробный алгоритм реализации программного средства защиты.

Ключевые слова: модемы, исполнительная программа, несанкционированный доступ, информационная безопасность, криптографические примитивы.