МОДЕЛЬ ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В РЕГИОНАЛЬНОМ ИНТЕРНЕТ-ПРОСТРАНСТВЕ ДЛЯ СЕТИ FACEBOOK

А.Г. Остапенко, А.В. Ещенко, Г.А. Остапенко, К.В. Симонов

В статье приведено исследование основных признаков деструктивности контента, а также реакции Интернет-пользователей на просмотренный негативный контент в социальной сети Facebook.

Ключевые слова: социальная сеть, деструктивный контент, сетевая модель, Facebook.

МЕТОД ЭФФЕКТИВНОГО РАСПРЕДЕЛЕНИЯ СКАНЕРОВ ДЛЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЗЛОВ ГЕТЕРОГЕННОЙ СЕТИ

А.О. Калашников, Е.В. Аникина

В работе рассматривается один из методов эффективного распределения ограниченного ресурса специализированных устройств (сканеров) для мониторинга информационной безопасности узлов гетерогенной сети.

Ключевые слова: гетерогенная сеть, мониторинг информационной безопасностью, сканер безопасности, распределение ресурса.

МОДЕЛЬ ПРОГНОЗИРОВАНИЯ РИСКОВОГО ПОТЕНЦИАЛА ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

А.О. Калашников, Е.А. Сакрутина

В работе рассматривается модель прогнозирования рискового потенциала для системы мониторинга угроз безопасности выхода технологического процесса на аварийные режимы на значимых объектах критической информационной инфраструктуры.

Ключевые слова: критическая информационная инфраструктура, значимый объект критической информационной инфраструктуры, оценка рискового потенциала, ассоциативный поиск.

ПРИМЕНЕНИЕ DLP-СИСТЕМЫ SEARCHINFORM ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЕТИ INTERNET

П.Ю. Филяк, В.И. Старченко, А.В. Царегородцев, С.Х.У. Рашидов

В статье рассматривается подход к обеспечению информационной безопасности в сети Internet на основе использования DLP-системы (Data Leakage Prevention средствами System) - готовых программных решений компании SearchInform. Представлен подход к решению проблемы и некоторые возможности.

Ключевые слова: информационная безопасность, данные, информация, утечки, предотвращение утечек, системы предотвращения утечек данных, DLP-system.

МОДЕЛИ ПОСТРОЕНИЯ И ВБРОСА ДЕСТРУКТИВНОГО КОНТЕНТА В РЕГИОНАЛЬНОМ ИНТЕРНЕТ-ПРОСТРАНСТВЕ ЧЕРЕЗ СОЦИАЛЬНУЮ СЕТЬ ДЛЯ ОБМЕНА МЕДИА-КОНТЕНТОМ YOUTUBE

Ю. Штефанович, Ю.О. Гончаров, Д.А. Савинов, Н.И. Баранников, И.Л. Батаронов, В.В. Исламгулова

В статье описываются модели построения деструктивного контента, включая нахождение его шаблонов, оценки эмоций, которые влияют на вирусность контента, а также основных параметров целевой аудитории, влияющих на скорость распространения контента.

Ключевые слова: информационные сети, социальные сети, деструктивный контент, вброс, построение, Youtube.

ИНТЕРНЕТ - БЕЗОПАСНОСТЬ ПУТЕМ СОЗДАНИЯ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО АУДИТА С ПОМОЩЬЮ СКРИПТОВОГО ЯЗЫКА "AUTOIT"

П.Ю. Филяк, В.И. Старченко

В статье рассматривается подход к обеспечению безопасности в сети Интернет с помощью использования подходов и сертифицированных инструментальных средств защиты информации, которые начали применяться для обеспечения информационной безопасности как совсем недавно, так и на протяжении длительных сроков, и уже успели зарекомендовать себя в качестве надежных проверенных средств. Отличие подходов заключается в применении для аудита событий информационной безопасности известных решений в сочетании со средой автоматизации, для создания которой предложено использовать скриптовый язык AutoIt.

Ключевые слова: интернет, информация, безопасность, безопасность информации, информационная безопасность, инструментальные средства, средства защиты информации, автоматизация, программирование, скриптовый язык, скриптовый язык Autolt.

АЛГОРИТМЫ ПРОТИВОБОРСТВА В ХОДЕ СТОЛКНОВЕНИЯ ТЕКСТОВЫХ КОНТЕНТОВ В ИНТЕРНЕТ-СООБЩЕСТВАХ

Е. Ружицкий, Е.В. Труфанов, Ю.Н. Гузев, Н.И. Баранников, А.В. Заряев, К.В. Симонов

В статье описываются алгоритмы противоборства в автоматизированной социальной сети ВКонтакте, способствующие выявлению назревающих конфликтных ситуаций с целью дальнейшего принятия тактических и стратегических действий для их разрешения между противоборствующими Интернет-сообществами, а также построение модели противоборства, на основе которой можно получить более точную картину взаимодействия пользователей противоборствующих Интернет-сообществ.

Ключевые слова: виртуальное сообщество, текстовый контент, пользователь, подписчик, противоборство, алгоритм, модель, ВКонтакте.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ НА ОСНОВЕ СЕРТИФИЦИРОВАННЫХ РЕШЕНИЙ ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ/АТАК

П.Ю. Филяк, Ю.Н. Данилова, Н.В. Гришина, А.М. Найль

Рассматривается решение проблем обеспечения информационной безопасности в сети Интернет на основе сертифицированных решений, предлагаемых разработчиками в качестве инструментов, позволяющих обеспечить комплексный подход к защите информации. Решения предлагаются на основе оценки уязвимостей сети и имитации реальных атак.

Ключевые слова: информационная безопасность, информационно-телекоммуникационная сеть, уязвимость, мониторинг, атака/вторжение, сканер безопасности, логирование.

ПОТЕНЦИАЛ ВИДЕОРОЛИКОВ СЕТИ YOUTUBE ДЛЯ РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В РЕГИОНАЛЬНОМ ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Й. Воришек, Д.А. Савинов, К.С. Фадин, Н.И. Баранников, И.Л. Батаронов

В статье рассматривается процесс распространения деструктивного контента с учетом особенностей сети YouTube, а также факторы, влияющие на продвижение видеоролика. Рассмотрены качества контента, которые воздействуют на сознание пользователя. И с учетом структурных и функциональных возможностей социальной сети YouTube рассматриваются условия возникновения этих качеств. Также были рассмотрены существующие метрики контента и предложены новые оценки потенциала видеоролика, которые могут помочь определить, какие ролики могут иметь наибольшее распространение, в зависимости от скорости изменения метрик в первые несколько часов с момента публикации видео на канале. Материалы

статьи представляют практическую ценность для специалистов в области мониторинга социальных сетей, ставших ареной ожесточенной битвы деструктивных контентов в мировом мультисетевом пространстве.

Ключевые слова: социальная сеть Youtube, модель распространения, деструктивный контент, интернет-сообщества, метрики контента.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В ИНТЕРНЕТ НА ОСНОВЕ АНАЛИЗА С ИСПОЛЬЗОВАНИЕМ СЕРТИФИЦИРОВАННЫХ РЕШЕНИЙ MAX PATROL

П.Ю. Филяк, Э.Э. Байларли, И.Н. Мухин, У.Ж.У. Ибрагимов

Рассматривается информационная безопасность автоматизированных систем как в автономном режиме, так и в случае интеграции в глобальную сеть Интернет, с помощью программного продукта MaxPatrol от компании PositiveTechnologies. MaxPatrol обеспечивает комплексный мониторинг информационной безопасности предприятия, решая такие задачи, как контроль эффективности процессов информационной безопасности, политик безопасности и их изменения, инвентаризация и оценка защищенности.

Ключевые слова: информационная безопасность, интернет, автоматизированная система, аудит безопасности, угроза безопасности информации, защищенность.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ЧЕРЕЗ ИНТЕРНЕТ

Н.С. Егошин, А.А. Конев, А.А. Шелупанов

В статье приводится обоснование необходимости разработки новой единой модели угроз безопасности информации. Проводится сравнение и анализ существующих моделей. Обосновывается необходимость применения модели информационных потоков системы. Предлагается своя собственная модель угроз, в основе которой лежит модель информационных потоков.

Ключевые слова: информационная безопасность, информационные потоки, модель угроз.

ОБЪЕКТНО-ОРИЕНТИРОВАННОЕ ПРОГРАММИРОВАНИЕ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

П.Ю. Филяк, В.В. Растворов, Н.В. Гришина, А.М. Найль

В статье рассматривается объектно-ориентированное программирование (ООП) как способ обеспечения информационной безопасности в сетях, и в сети Интернет в частности, путем контроля обработки данных и доступа к данным.

Ключевые слова: безопасность, сеть, безопасность сети, доступ, объективн-ориентированное программирование, разграничение доступа, защищенность.

ОБНАРУЖЕНИЕ ПРОГРАММ-БОТОВ В СОЦИАЛЬНЫХ СЕТЯХ НА ОСНОВЕ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

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

Данная статья посвящена анализу проблемы распространения ботов в социальных сетях. В работе описываются и сравниваются технологии применения нейронной сети, дерева решений и логистической регрессии для решения задачи обнаружения ботов в социальных сетях. Оцениваются адекватность и эффективность классификации пользователей информационной системы с помощью построенных моделей.

Ключевые слова: бот, твит, репост, нейронная сеть, дерево решений, логистическая регрессия.

ПОДХОДЫ И ИНСТРУМЕНТЫ "ELCOMSOFT" - ДЛЯ БЕЗОПАСНОГО ИНТЕРНЕТА

П.Ю. Филяк, В.В. Растворов, И.Н. Мухин, С.Х.У. Рашидов

В статье рассматривается подходы и инструменты - для безопасного интернета на базе политики парольной защиты путем анализа устойчивость по отношению к атакам на локальные сети и сети wi-fi - посредством использования продуктов компании ElcomSoft.

Ключевые слова: безопасность сети, автоматизированная система, парольная защита, атака, стойкость пароля, защищенность.

АНАЛИЗ И КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНЫХ СЕТЕВЫХ ОПЕРАЦИЙ

А.С. Пахомова, А.П. Пахомов, В.И. Белоножкин, В.Г. Юрасов, К.В. Симонов

В статье рассматриваются новые понятия, относящиеся к области конфиденциальных сетевых операций. Выделяются основные признаки методов защиты информации от угроз, возникающих при легитимном сетевом информационном взаимодействии. Предлагается классификация конфиденциальных сетевых операций по видам защищаемых данных и дается характеристика реализуемости существующих методов защиты.

Ключевые слова: конфиденциальные сетевые операции, многосторонние вычисления, гомоморфное шифрование, конфиденциальный поиск данных.

БЕЗОПАСНЫЙ ИНТЕРНЕТ - ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ДЛЯ УПРАВЛЕНИЯ АНТРОПОГЕННЫМИ РИСКАМИ

П.Ю. Филяк, С.Н. Федирко, Д.А. Рычков, М.О. Бартов, В.В. Гузей, Т.М. Султанов

Рассматриваются подходы и инструментальные средства для обеспечения информационной безопасности, оценки угроз и противодействия им в целях избежания или минимизации возможных рисков, связанных с действиями человека (антропогенными рисками) при использовании сети Интернет.

Ключевые слова: интернет, информация, угрозы, риски, средства защиты информации (СЗИ), антропогенные риски.

ОБ ОПТИМИЗАЦИОННОМ АЛГОРИТМЕ ИНФОРМАЦИОННОГО ПОИСКА С УЧЕТОМ РИСКА РАЗГЛАШЕНИЯ ИНФОРМАЦИИ

А.П. Пахомов, А.С. Пахомова, Л.В. Паринова, Н.Н. Толстых, К.В. Симонов

В статье излагаются математические основы оптимизационного алгоритма информационного поиска с учетом риска разглашения информации в процессе запроса данных из различных источников. Оптимизационный алгоритм обоснован путем формулирования задачи информационного поиска как задачи минимизации многомерного пути наслучайном графе.

Ключевые слова: оптимизация пути поиска, риск разглашения, конфиденциальное извлечение.

ПРИМЕНЕНИЕ INFOWATCH DLP-СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЕТИ INTERNET

П.Ю. Филяк, С.Н. Федирко, А.В. Царегородцев, У.Ж.У. Ибрагимов

В статье рассматривается подход к обеспечению информационной безопасности корпоративной сети на основе использования DLP-системы (Data Leakage Prevention средствами System) - готовых технических решений компании InfoWatch. Представлены подход к решению проблемы и некоторые результаты.

Ключевые слова: информационная безопасность, данные, информация, утечки, системы предотвращения утечек данных, DLP-system, сеть интернет.

О МОДЕЛИ УГРОЗЫ РАЗГЛАШЕНИЯ ИНФОРМАЦИИ ЧЕРЕЗ ОБРАЩЕНИЕ К ЛОГИЧЕСКИ СВЯЗАННЫМ ДАННЫМ В ПРОЦЕССЕ ИНФОРМАЦИОННОГО ПОИСКА

А.П. Пахомов, А.С. Пахомова, Н.Н. Толстых, В.Г. Юрасов, К.В. Симонов

В статье рассматривается модель угрозы разглашения информации, которая может быть реализована в процессе информационного поиска через обращение к логически связанным данным. Для обоснования модели использованы разработки сходных по назначению моделей, предназначенных для оценки риска распространения прав доступа в автоматизированных системах (модель Take-Grant) и риска распространения информации о кибербезопасности.

Ключевые слова: безопасность информации, разглашение, распространение информации, модель, риск.

ИСПОЛЬЗОВАНИЕ АНАЛИТИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ ОПИСАНИЯ ДИНАМИЧЕСКОГО РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНЫХ СЕТЯХ

А.В. Паринов

В статье рассматривается вопрос использования аналитических моделей исследования эпидемических информационных процессов в онлайновых социальных сетях, которые являются взвешенными неоднородными сетями.

Ключевые слова: социальные сети, деструктивный контент, ущерб, риски, дискретная модель.

ЦЕНООБРАЗОВАНИЕ В СИСТЕМЕ ГОСУДАРСТВЕННЫХ ЗАКУПОК ГОРОДА МОСКВЫ КАК ВАЖНЫЙ КЛАСТЕР ПОСТРОЕНИЯ ОТЕЧЕСТВЕННОЙ ЦИФРОВОЙ ЭКОНОМИКИ

А.Ф. Белый, В.Р. Григорьев, А.В. Кочергин

Создание технологий цифровой экономики напрямую связано с решением вопросов экономической и информационной безопасности. Рассмотрены вопросы управления ценообразованием в качестве практической основы системных решений по организации отечественной цифровой экономики и предотвращения системных издержек в результате наложенных на Россию экономических санкций. Поставлен вопрос о создании системы подготовки принципиально новых кадров в области ценообразования в условиях построения цифровой экономики.

Ключевые слова: информационная экономика, информационное противоборство.

СОЦИАЛЬНЫЕ СЕТИ - ИНСТРУМЕНТ СЕТЕВОГО ПРОТИВОБОРСТВА В ГИБРИДНОЙ ВОЙНЕ

В.Р. Григорьев

В связи с быстрым развитием средств коммуникации информационный фактор в настоящее время играет всё более существенную роль при обеспечении различными государствами своих геополитических интересов. Технологии ведения информационных войн с помощью социальных инструментов сети Интернет оказывают массированное информационно-психологическое воздействие на мировое сообщество с целью формирования благоприятного общественного мнения. В статье исследуется место социальных сетей в структуре современной гибридной войны.

Ключевые слова: социальные сети, информационно-психологические воздействия.

СОЦИАЛЬНЫЕ СЕТИ: МОДЕЛИРОВАНИЕ ДИНАМИКИ РАСПРОСТРАНЕНИЯ МАНИПУЛЯТИВНЫХ ВОЗДЕЙСТВИЙ

В.А. Минаев, Е.В. Вайц, А.Э. Киракосян, В.В. Умеренков

В статье рассмотрена базовая системно-динамическая модель распространения манипулятивных информационных воздействий в социальных сетях, включая идеи экстремизма. Проведена ее реализация в имитационной среде моделирования Anylogic, описаны результаты некоторых имитационных экспериментов с моделью.

Ключевые слова: системно-динамическое моделирование, манипулятивное информационное воздействие, социальная сеть, имитационная среда.