ВЛИЯНИЕ НОВЫХ ТЕХНОЛОГИЙ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

А.О. Калашников, Е.В. Аникина, Г.А. Остапенко, В.И. Борисов

В работе рассматриваются новые информационные технологии и их влияние на информационную безопасность объектов критической информационной инфраструктуры Российской Федерации и критической информационной инфраструктуры в целом.

Ключевые слова: информационные технологии, информационная безопасность, критическая информационная инфраструктура.

ОСНОВЫ МЕТРОЛОГИИ КОНТЕНТОВ ДЛЯ МОНИТОРИНГА СОЦИАЛЬНЫХ СЕТЕЙ НА ПРЕДМЕТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЧАСТЬ 1)

А.Г. Остапенко, Е.С. Соколова, А.В. Ещенко, А.А. Остапенко, Т.Ю. Чапурина

В работе рассматриваются атаки с помощью деструктивных контентов. Особое внимание уделяется пользователям социальных автоматизированных сетей, которые являются конечным объектом этих атак. В этой связи авторами предлагается серия аналитических выражений, учитывающая мощности множеств пользователей с различной реакцией на деструктивный контент. При достаточной общности предлагаемой методики акцент сделан на региональный аспект. Все это в совокупности образует риск-модель, которая может служить методической основой для принятия решений по противодействию атакам социальных сетей посредством деструктивного контента.

Ключевые слова: социальная сеть, деструктивный контент, риск, мониторинг.

ОСНОВЫ МЕТРОЛОГИИ КОНТЕНТОВ ДЛЯ МОНИТОРИНГА СОЦИАЛЬНЫХ СЕТЕЙ НА ПРЕДМЕТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЧАСТЬ 2)

А.Г. Остапенко, Е.С. Соколова, А.В. Ещенко, А.А. Остапенко, Т.Ю. Чапурина

Рассматриваются атаки сети деструктивным контентом. Внимание уделяется пользователям социальных сетей, которые являются объектом этих атак. Авторами предлагаются аналитические выражения, учитывающие мощности множеств пользователей с различной реакцией на деструктивный контент. Акцент сделан на региональный аспект. Все это в совокупности образует риск-модель, которая может служить методической основой для принятия решений по противодействию атакам на социальные сети посредством деструктивного контента.

Ключевые слова: социальная сеть, деструктивный контент, риск, мониторинг.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ МОНИТОРИНГА ПРОЦЕССОВ ВОСПРИЯТИЯ И РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНЫХ КОНТЕНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

А.Г. Остапенко, Е.Ю. Чапурин, Е.С. Соколова, А.Г. Зимницкий, И.А. Боков, С.В. Лихобабин, А.О. Ткаченко, А.И. Дегтярев

В работе рассматриваются принципы разработки автоматизированной системы выявления и исследования деструктивного контента социальных сетей «Вконтакте» и «Одноклассники». Реализованная в настоящем исследовании разработка прикладного программного обеспечения открывает возможности для дальнейшего изучения сетевого пространства и рисков, связанных с деструктивной деятельностью пользователей как внутри, так и вне виртуального мира.

Ключевые слова: социальная сеть, деструктивный контент, риск.

РЕГИОНАЛЬНЫЙ РЕЕСТР КОНТЕНТОВ: РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.Г. Титов, Е.Ю. Чапурин, Е.С. Соколова, М.Е. Волкова, Д.С. Хохлова

Рассматривается проблема защиты реестра деструктивных контентов, создаваемого в рамках проекта «Безопасный Интернет». В этой связи предлагаются рекомендации по снижению рисков информационной безопасности данного реестра в условиях реализации на него атак злоумышленников.

Ключевые слова: реестр, атака, злоумышленник, риск, защита.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ДОСТУПОМ С ПОМОЩЬЮ МОДЕЛЕЙ АНАЛИЗА СИСТЕМ ЗАЩИТЫ

П.Ю. Филяк, В.В. Растворов, С.С. Куликов, В.И. Белоножкин, М.И. Бочаров

В статье рассматриваются подходы, позволяющие автоматизировать управление политиками доступов и анализ их защиты с помощью моделей анализа систем защиты.

Ключевые слова: политика доступов, права доступов, автоматизированная система, модель, безопасность, система защиты, защищенность.

МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ОПРЕДЕЛЕНИЯ ВОЗМОЖНОСТИ ОПЕРЕЖЕНИЯ МЕРАМИ ЗАЩИТЫ ПРОЦЕССА РЕАЛИЗАЦИИ УГРОЗ

Ю.К. Язов, М.А. Тарелкин, И.О. Рубцова

В статье предложен новый показатель оценки эффективности защиты информации, направленный на определение возможности опережения мерами защиты процесса реализации угроз безопасности информации в информационных системах. Для расчета нового показателя разработана математическая модель процесса реализации угроз с использованием аппарата сетей Петри-Маркова в условиях применения мер защиты. Получены аналитические соотношения для расчета предложенного показателя.

Ключевые слова: показатель эффективности, функциональная модель, сеть Петри-Маркова, угроза безопасности, мера защиты.

ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ НЕГАРМОНИЧЕСКОГО ЭЛЕКТРОМАГНИТНОГО ПОЛЯ ПИКОСЕКУНДНОГО ДИАПАЗОНА ДЛИТЕЛЬНОСТЕЙ

И.Н. Зайцева, Н.А. Фортунова, П.Ю. Филяк, Д.О. Карпеев, Е.А. Москалева

В статье рассматривается подход к обеспечению информационной безопасности с помощью инженерно-технических методов защиты информации и, в частности, с помощью аппаратных средств защиты информации. Предложена теоретическая основа использования подхода, описаны математически основные количественные требования к предлагаемому техническому решению.

Ключевые слова: информационная безопасность, средства защиты информации, несанкционированный съем информации, несанкционированный доступ к информации, импульсный метод, радиосредства несанкционированного съема информации, зондирующие импульсы.

СПОСОБ ГЕОГРАФИЧЕСКОЙ ПРИВЯЗКИ ИЗОБРАЖЕНИЙ ЧЕРЕЗ ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ ПРОСТРАНСТВЕННЫХ ОБЪЕКТОВ ПРИ КОСМИЧЕСКОМ ДИСТАНЦИОННОМ ЗОНДИРОВАНИИ ЗЕМЛИ

А.В. Воронин, В.Н. Иванов

В статье рассматривается задача обеспечения безопасности географической привязки информации (изображений) в геоинформационных системах за счет разработки альтернативного способа определения параметров местоположения спутников дистанционного зондирования Земли. Способ основан на использовании измерения разницы времени прихода пакетов, содержащих специальные временные метки, с временными метками, вырабатываемых на наземных комплексах приема и обработки данных.

Ключевые слова: геоинформационная система, пространственный объект, местоположение, дистанционное зондирование земли, безопасность, информация.

ПРОЦЕДУРНОЕ ПРОГРАММИРОВАНИЕ В РАССЛЕДОВАНИЯХ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, В.В. Растворов, Н.М. Радько, Н.Н. Толстых

В статье рассматриваются подходы, позволяющие обеспечить оперативное реагирование на инциденты информационной безопасности с помощью базовых средств операционных систем и процедурного программирования.

Ключевые слова: информационная безопасность, инциденты информационной безопасности, программирование, резервная копия, реагирование на инциденты.

ИССЛЕДОВАНИЕ ПРОЦЕССА РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В СЕТИ INSTAGRAM ДЛЯ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ ВОРОНЕЖСКОЙ ОБЛАСТИ

И.А. Сурков, Р.А. Гриднев, В.В. Сафронова, К.В. Сибирко

В работе исследуется аудитория региональных пабликов Instagram для интернет-пользователей Воронежской области. Рассмотрены метрики, которые используются при анализе региональных пабликов и подписчиков. Предложена аналитическая модель для процесса распространения деструктивного контента в сети Instagram.

Ключевые слова: Instagram, паблик, метрики, деструктивный контент.

ГРАФОВАЯ МОДЕЛЬ ДИФФУЗИИ ДЕСТРУКТИВНОГО КОНТЕНТА С УЧЕТОМ «ПРОБЛЕМЫ ПЕРЕЗАЛИВОВ»

Е.Ю. Чапурин, В.В. Морковина, П.А. Анцупов, А.Н. Мокроусов

Предложена математическая модель распространения контента при активном механизме модерирования процессов для регионального сегмента социальной сети «ВКонтакте» с учетом «проблемы перезаливов» при распространении деструктивного контента в сообществах. Проведено сравнение активного механизма модерирования с пассивным. Модернизирована модель SEIR с учетом диффузий контентов и «проблемы перезаливов». Для данной модели предложен математический аппарат, позволяющий рассчитать вероятности атак деструктивным контентом на пользователей регионального сегмента социальной сети.

Ключевые слова: социальная сеть, деструктивный контент, риск.

АВТОМАТИЗАЦИЯ ПОИСКА РАСПРОСТРАНИТЕЛЕЙ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНЫХ СЕТЯХ

Д.А. Ишков, Е.Р. Нежельский, М.Н. Степанов

Статья посвящена проблеме безопасности Интернет-пространства, в частности социальной сети Instagram. Изложены возможные пути ее решения с целью построения программного обеспечения на основе приведенных в статье алгоритмов. Рассмотрены понятия «социальный капитал» и «потенциальная опасность блогеров», приведены формулы по их оценке. Предлагаемая схема автоматизации имеет полную независимость от разработчиков социальной сети, наличия API и ограничений по запросам.

Ключевые слова: Instagram, деструктивный контент, анализ, автоматизация, социальный капитал.

ОЦЕНКА ОПАСНОСТИ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНОЙ СЕТИ YOUTUBE

Ю.О. Гончаров, В.Д. Менжунов, В.Р. Носоленко

Для оценки опасности контента и канала его распространения используются эмоции, которые вызывает контент, и такие параметры канала распространения, как количество и длина контента, размер аудитории, лайки, дизлайки, пересечение аудиторий, количество контента созданного раньше, ключевые слова и тэги. Предложенные параметры и способ их оценки применимы в системах с высоким уровнем автоматизации для выявления наиболее вредоносных источников информации в социальных сетях для обмена медиа контентом.

Ключевые слова: социальная сеть, деструктивный контент, риск.

ОЦЕНКА ВЛИЯНИЯ СФЕРИЧНОСТИ ЗЕМЛИ НА КАЧЕСТВО ВИДОВОЙ ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ ПРИ ДИСТАНЦИОННОМ ЗОНДИРОВАНИИ ЗЕМЛИ ИЗ КОСМОСА

А.В. Бабурин, А.С. Пахомова, Т.Л. Тураева

Проводится уточнение эффективной ширины полосы обзора космического аппарата, оснащенного оптико-электронной аппаратурой, в пределах видимости которой обеспечивается заданное качество изображения.

Ключевые слова: космический аппарат, оптико-электронная аппаратура, линейное разрешение на местности.

К ВОПРОСУ О КЛАССИФИКАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

А.С. Пахомова, В.К. Власов, А.В. Паринов

Проводится сравнительный анализ правил классификации и категорирования автоматизированных систем в защищенном исполнении, предназначенных для различения требований по обеспечению безопасности информации, предъявляемых к этим системам.

Ключевые слова: автоматизированная система, безопасность, критерий, теория риска.

РАЗМЕЩЕНИЕ УЗЛОВ СЕТЕВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ С КОМБИНАТОРНОЙ ТОПОЛОГИЕЙ С ЦЕЛЬЮ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Ю.Ю. Громов, Ю.В. Минин, С.А. Копылов

В статье рассматривается вопрос размещения элементов сетевых информационных систем

для объектов, относящихся к критической информационной инфраструктуре, с целью повышения информационной безопасности в условиях неопределенности. Сформулированные оптимизационные задачи предназначены для синтеза сетевых информационных систем, обладающих комбинаторной топологией. Неопределенность и недостаточность информации о параметрах системы учтены за счет введения нечетких параметры в постановку задачи. Предложены алгоритмы решения поставленных задач для предельного случая.

Ключевые слова: сетевая информационная система, защита информации, неопределенность, нечеткость.

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ОБЪЕКТА АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.А. Воеводин

Обладатель информации обязан принять меры по защите информации. Эффективность принимаемых решений зависит от полноты, достоверности и своевременности информации, которая добывается в ходе аудита ИБ. В настоящее время аудит ИБ осуществляется на основе обобщения эмпирических знаний и опыта, которые закреплены в практических рекомендациях и стандартах, достижения фундаментальной науки для этих целей применяются не в полной мере. Приведена концептуальная модель объекта аудита ИБ и формальные постановки задач: вывода аудиторского доказательства и преобразования аудиторских доказательств в аудиторское заключение, приведены рекомендации по применению результатов и направления дальнейшего исследования.

Ключевые слова: аудит информационной безопасности, аудиторский риск, аудиторское свидетельство, аудиторское доказательство, аудиторское заключение.