КАРТОГРАФИЧЕСКИЙ ПОДХОД В БИБЛИОМЕТРИЧЕСКОМ ИССЛЕДОВАНИИ ОТЕЧЕСТВЕННЫХ НАУЧНЫХ ШКОЛ, СЛОЖИВШИХСЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.О. Калашников, А.Л. Сердечный, А.Г. Остапенко

Целью исследований является определение состава отечественных научных школ в области защиты информации и обеспечения информационной безопасности для выявления творческих коллективов, способных решать сложные научные проблемы, а также для получения исходных данных и инструментов, необходимых для дальнейших исследований состояния и тенденций развития данной предметной области. В работе продемонстрирован картографический подход к решению задачи выявления научных сообществ на примере построения и анализа библиометрической сети соавторов научных публикаций в области защиты информации и обеспечении информационной безопасности, который может быть применён для решения аналогичных задач в других предметных областях. Построена интерактивная карта научных школ в области защиты информации и обеспечения информационной безопасности, позволяющая наглядно представить состав и границы научных объединений и их творческие взаимосвязи. При помощи интерактивной карты были выявлены наиболее крупные научные объединения. Полученные результаты могут быть использованы как исследователями вопросов защиты информации и обеспечения информационной безопасности для поиска научных публикаций по теме, так и руководителями проектов для обеспечения научного взаимодействия с подходящими коллективами при решении сложных научных проблем.

Ключевые слова: научные школы, библиометрическая сеть соавторов, защита информации, информационная безопасность, картографический подход, картография киберпространства.

ОБРАЗОВАНИЕ КАК ИНСТРУМЕНТ ИНФОРМАЦИОННОЙ ВОЙНЫ

А.А. Малюк, В.А. Минаев, М.П. Сычев

Статья посвящена проблеме использования образовательной среды в качестве инструмента ведения информационных войн. При этом образование включает систему образовательных учреждений, средства массовой информации, процесс самообучения. Понятие “информационная война” раскрывается как современное оружие массового поражения, используемое для манипулирования общественным мнением в целях достижения негативных результатов применительно к противнику. Проводится анализ образования как сферы деятельности, подверженной воздействию информационного оружия. Раскрывается политика образования как социокультурный феномен, потенциально имеющий уязвимости перед информационным оружием. Описана и рассмотрена вербальная модель информационных процессов, реализуемых социальным субъектом, а также методы воздействия на эти процессы, лежащие в основе информационных войн. Осуществляется анализ этих методов, и приводятся реальные примеры их применения. Отмечается решающая роль информационной культуры общества в решении задач противодействия использованию образования в качестве инструмента информационной войны. Рассматривается глобальный аспект культуры информационной безопасности. Делается вывод, что для противодействия угрозам использования инструментов образования для ведения информационных войн высоко актуальна проблема формирования в обществе, особенно у молодого поколения, культуры информационной безопасности.

Ключевые слова: образование, информационная война, манипулирование массовым сознанием, культура информационной безопасности.

ИНФРАСТРУКТУРА КАК КОД: ФОРМИРУЕТСЯ НОВАЯ РЕАЛЬНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.О. Калашников, К.А. Бугайский

В настоящей статье проведен анализ появления и развития облачных, туманных и периферийных вычислений. Показано, что данные типы вычислений с одной стороны базируются, а с другой стороны - способствуют активному развитию трех базовых инфраструктурных технологий – архитектуры микросервисов, виртуализации (в том числе контейнерной) и программно-определяемых сетей. Симбиоз этих технологий, в свою очередь,

привел к появлению и развитию понятия «Инфраструктура как Код». Построение информационных систем на основе подхода «Инфраструктуры как Код» предполагает, что создание и взаимодействие компонент информационной инфраструктуры осуществляется с помощью интерфейсов прикладного программирования и файлов конфигурации. Использование интерфейсов прикладного программирования и файлов конфигурации для формирования информационной инфраструктуры повышает адаптационные способности информационных систем. Необходимо отметить, что в настоящее время информационная инфраструктура уже должна рассматриваться как «Cloud-Fog-Edge», то есть как симбиоз и естественный результат развития облачных, туманных и периферийных вычислений. Соответственно, расширяется и наполнение термина «Инфраструктура как Код», которое в ближайшие несколько лет будет формировать новые аспекты информационной безопасности в вычислительных системах, в том числе, относящихся к объектам критической информационной инфраструктуры Российской Федерации.

Ключевые слова: инфраструктура как код, информационная безопасность, микросервисы, виртуализация.

КВАНТОВЫЕ ТЕХНОЛОГИИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, А.Н. Ермолин

Квантовая криптография в настоящее время рассматривается как сравнительно новый и, пожалуй, самый перспективный метод криптографической защиты. Предложена наглядная интерпретация достаточно сложного метода инженерно-технической защиты информации, который в отличие от методов традиционной математической криптографии, требует оперирования определенными абстрактными категориями, которым очень важно дать некую их иллюстрацию, необходимую для понимания данной тематики – что такое квант, спин, суперпозиция, квантовое состояние, кубит, протокол шифрования, фотон, интерференция, квантовая запутанность и другие.

Ключевые слова: информационная безопасность, сертификат ключа проверки электронной подписи, криптография, квантовая криптография.

МОДЕЛИ КОЛИЧЕСТВЕННОГО ОЦЕНИВАНИЯ КОМПЬЮТЕРНЫХ АТАК (ЧАСТЬ 1)

А.О. Калашников, К.А. Бугайский, Е.В. Аникина

В настоящей статье на основании анализа экспертных материалов по информационной безопасности сделан ряд предложений по оцениванию компьютерной атаки как процесса, управляемого со стороны нарушителя – атакующего субъекта. Цель данной работы состоит в разработке моделей, позволяющих получить описание цели управления процессом атаки со стороны атакующего субъекта, последовательности действий атакующего субъекта, включая выбор инструментов атаки, количественных оценок объекта атаки, которые может использовать субъект атаки при выборе объекта для проведения атаки. Развитие компьютерной атаки рассматривается как последовательность этапов реализующихся во времени и пространстве – в топологии подвергающейся атаке информационной системы. В рамках предложенного подхода разработаны модели компьютерных атак, позволяющие проводить количественную оценку состояния как объекта атаки, так и действий атакующего субъекта. Указанная оценка может быть реализована, в том числе динамически – на каждом из этапов развития атаки и в отношении каждого из атакуемых элементов информационной системы (например, средств вычислительной техники). Сформулированы положения для построения модели объекта атаки.

Ключевые слова: компьютерная атака, информационная безопасность, модель, информационная система, средство вычислительной техники.

МОДЕЛИ КОЛИЧЕСТВЕННОГО ОЦЕНИВАНИЯ КОМПЬЮТЕРНЫХ АТАК (ЧАСТЬ 2)

А.О. Калашников, К.А. Бугайский, Е.В. Аникина

Рассмотрены методы количественного оценивания вероятности успешных действий субъекта атаки, а также последовательности его действий, необходимые для модели объекта атаки. Представлено формализованное описание объекта атаки. Представлены алгоритмы этапов моделирования процессов проведения атаки. Рассмотрены вопросы устойчивости информационной системы в условиях проведения атак. Показано, что разработанные модели предоставляют исходные данные для расчетов эффективного распределения затрат на реализацию мер информационной безопасности в информационных системах на основе механизмов теоретико-игрового и стохастического моделирования и специально разработанных алгоритмов. Предложенные модели также позволяют разработать алгоритмы и методы количественных оценок эффективности применения средств защиты информации на всех этапах жизненного цикла информационной системы, в том числе, этапе ее проектирования.

Ключевые слова: компьютерная атака, информационная безопасность, модель, информационная система, средство вычислительной техники.

ОБ ОДНОМ ИЗ АСПЕКТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

П.Ю. Филяк, В.В. Пименова, А.Н. Ермолин

В настоящее время наблюдается бурное развитие средств массовой информации (СМИ) и уже не столько в традиционно привычном сегменте, пресса, радио, телевидение, сколько в новых формах и с применением новых информационных и информационно-коммуникационных технологий (ИКТ), на основе, в частности широкого использования информационно-телекоммуникационных сетей (ИТКС), по проводному либо беспроводному принципу передачи данных, как с использованием протоколов сети Internet, как глобальной информационной среды, так и на основе иных коммуникаций. Тем не менее, вся система вселенского эфира, как ни странно это может показаться, держится на тонкой ножке квалификации представителей СМИ и вещательных организаций, от профессионализма которых с учетом масштабов современного информационного пространства зависят глобальные не только информационные, но и социальные процессы.

Ключевые слова: информация, информационные технологии, интерфейс, web-интерфейс, информационная безопасность.

РАЗВИТИЕ АВТОМАТНЫХ МОДЕЛЕЙ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ ОБЪЕКТОВ

А.О. Калашников, А.Ю. Максимовский

Мониторинг информационной безопасности сложных систем, в том числе с сетевой структурой является одним из наиболее эффективных инструментов обеспечения их надежного функционирования. В качестве критериев, используемых при осуществлении мониторинга сложных систем, как правило, выступают характерные особенности их внешнего поведения. Примерами таких особенностей являются, например, запреты определенных выходных последовательностей указанных сетевых объектов, представленных автоматными моделями. В предыдущих работах авторов в качестве механизмов для выявления особенностей внешнего поведения объектов контроля были предложены 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 графах или мультиграфах состояний соответствующих автоматов). При этом, в качестве автоматных моделей рассматривались регистры сдвига или их обобщения, обладающие необходимыми свойствами для целей осуществления мониторинга информационной безопасности сетевых объектов. В настоящей работе на базе расширения алгебраических структур предложено развитие моделей мониторинга информационной

безопасности объектов сетевой инфраструктуры, основанная на контроле алгебраических и комбинаторных соотношений входных и выходных последовательностей указанных объектов.

Ключевые слова: мониторинг информационной безопасности, конечный автомат, регистр сдвига, диаметр графа.

МОНИТОРИНГ И УПРАВЛЕНИЕ РИСКАМИ СОЦИО-ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ РЕГИОНАЛЬНОЙ И НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А.Г. Остапенко, В.П. Железняк, Е.Ю. Чапурин, А.А. Остапенко, С.Д. Трубицын, О.А. Остапенко, Т.Ю. Мирошниченко

Анализируется опыт государственного регулирования Интернет-пространства путем минимизации информационных рисков в целях обеспечения безопасности социума. На примере достижений Китайской Народной Республики исследуются наиболее радикальные средства информационного противоборства, достоинства и недостатки их применения. Формулируются (вытекающие из вышеуказанного анализа) задачи регионального мониторинга онлайн-сообществ. Конкретно в работе анализируется исторически сложившаяся организационно-управленческая парадигма Китая как модели гигантского муравейника, где единым старшим по положению является действующая власть и в соответствии с философией конфуцианства всякий гражданин обязан преодолевать своекорыстие во имя самосовершенствования на благо родины. Все это создает философско-историческую основу для введения и функционирования глубокого и масштабного контроля населения через информационные мониторинг и управление. В этой связи анализируется файервол «Золотой щит» и другие средства, ограничивающие внедрение нежелательного для правительства контента. Рассматривается также специфика системы социального кредита, фактически обеспечивающая неусыпное наблюдение за гражданами и их социальное категорирование. Армия троллей ограниченно дополняет вышеизложенное как активная составляющая противодействия политическим оппонентам. С учетом того, что рассмотренные информационные технологии находят сбыт в целом ряде стран, утверждается актуальность мониторинга социо-информационного пространства не только на национальном, но и на региональных уровнях. В этом контексте предлагаются структурно-функциональные технические решения по исследованию Интернет-пространства региона по реакциям его пользователей на резонансные контенты.

Ключевые слова: фильтр, социальная сеть, риск, безопасность, контент, троллинг.

СТРУКТУРНО-ФУНКЦИОНАЛЬНАЯ ФОРМАЛИЗАЦИЯ ПРОЦЕДУР РИСК-МОНИТОРИНГА РЕГИОНАЛЬНЫХ ПАБЛИКОВ

В.П. Железняк, Е.Ю. Чапурин, И.А. Боков, А.Г. Зимницкий, С.В. Лихобабин, А.О. Ткаченко, М.Н. Степанов

С учетом достигнутых результатов и тенденций развития инструментария мониторинга социальных сетей рассмотрены схемы параллельного и последовательного сканирования пабликов. Предложены блок-схемы алгоритмизации основных процедур мониторинга: сканирование, выявление и измерение контентов, а также формат данных и структура пользования базой выявленных деструктивных контентов. Конкретно в работе рассматриваются случаи, когда набор средств вычислительной техники (СВТ) позволяет реализовать параллельное наблюдение за пабликами, а также более экономичный вариант, когда обход пабликов осуществляется СВТ последовательно. Обобщенную структуру мониторинга предлагается организовать через два цикла по: перечню исследуемых пабликов и шагам мониторинга. При этом последовательно включаются модули: сканирования пабликов и выделения контентов, выявления и классификации деструктивных контентов, измерения и визуализации параметров и характеристик выявленных контентов, формирования базы данных. Формализация процесса сканирования предусматривает процедуры: извлечения поста и оценку его популярности, передачу поста на другие модули анализа с последующим внесением последнего в формируемую базу данных. После модуля сканирования процесс выявления деструктивного поста обеспечивает сравнение последнего с заданными признаками. В свою очередь метрический модуль решает задачи измерения параметров и характеристик выявленного поста в период его жизни по шагам мониторинга. В работе также предлагается формат создаваемой базы данных, а также организационная структура пользования последней в

регионе. Предложенные в работе формализмы могут быть положены в основу алгоритмизации и программной реализации соответствующего комплекса автоматизации мониторинга региональных пабликов на предмет исследования диффузии резонансных контентов.

Ключевые слова: деструктивный контент, алгоритмы, мониторинг, социальные сети, паблики, база данных.

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И БОЛЬШИХ ДАННЫХ ПРИ РЕАЛИЗАЦИИ РИСК-МОНИТОРИНГА РЕГИОНАЛЬНОГО СОЦИО-ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Г.А. Остапенко, Е.А. Москалева, Е.Ю. Чапурин, А.А. Остапенко, М.Е. Волкова, Д.С. Хохлова, Т.Ю. Мирошниченко

Коммуникация является важнейшим типом активного общения. Вместе с полезной, истинной информацией передается и ложная и деструктивная информация, формируемая в том числе преднамеренно. В современном социо-информационном пространстве, например, в социальных сетях, мы имеем распространение конструктивного и деструктивного контентов. Обращается особое внимание на региональный аспект этой проблемы. Анализируются наиболее популярные тенденции создания технологических платформ для анализа состояния и трендов развития регионального социо-информационного пространства. В частности, рассматриваются особенности использования инструментария больших данных в текстовой аналитике контентов (на лексическом, морфологическом, синтаксическом, семантическом и дискурсивном уровнях). Особенно перспективным представляется развитие и внедрение методологии и классификации контентов с использованием инструментов машинного обучения при обработке данных контент-мониторинга (интеллектуализация текстовой аналитики). В этой связи основой глубокой аналитики регионального социо-информационного пространства рассматриваются базы знаний, аккумулирующие логико-структурированные сведения для получения выводов о состоянии, тенденциях и временных характеристиках исследуемого пространства (логические, семантические, продукционные и фреймовые базы знаний). Вышеперечисленные базы знаний рассматриваются как «пища» для систем искусственного интеллекта (логические, нейроподобные, DataMining), возможность использования которых анализируется в контексте мониторинга и исследования социальных медиа, как разносчиков деструктивного контента. Предлагаются соответствующие программы исследовании на региональном уровне.

Ключевые слова: контент, риск, база знаний, большие данные, системы искусственного интеллекта.

ОРГАНИЗАЦИЯ МОНИТОРИНГА СОЦИО-ИНФОРМАЦИОННОГО ПРОСТРАНСТВА И ПОСТРОЕНИЕ МОДЕЛИ РЕГИОНАЛЬНОГО ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЯ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ЕГО БЕЗОПАСНОСТИ

Е.А. Шварцкопф, Д.А. Савинов, С.М. Пасмурнов, Е.Р. Нежельский, С.С. Тихонова, Н.М. Лантюхов, А.Н. Бартенев

В данной публикации рассматривается алгоритм электронного опроса респондентов для получения точной модели Интернет-пользователя. Для сбора информации о поведении интернет-пользователей используются как традиционные опросные методы, так и статистические данные. При использовании опросных методов всегда есть вероятность умалчивания респондентом каких-либо предпочтений, возможность забывания им чего-либо и т. п. Однако и статистические данные не всегда корректны. Так, высокая продолжительность нахождения на сайте может быть вызвана как интересным контентом, так и сложной манерой подачи материала или же вовсе отлучением индивида от монитора компьютера; имеются сложности с идентификацией пользователя и т. п. В связи с этим наиболее правильный подход - комбинирование опросов и анализа статистических данных. Основная концепция заключается в том, что выполняется рандомизация ключевых блоков вопросов. Это позволяет плавно распределить ключевые точки опроса без необходимости прохождения полного списка вопросов каждым респондентом. Далее система обработки результатов опроса сопоставит ответы и индивидуальные характеристики каждого респондента. После чего данные результаты позволят

выявить наиболее незащищенных пользователей Интернет-сети на территории Воронежской области Российской Федерации.

Ключевые слова: соцсети, контент, пользователь, респондент.

К ВОПРОСУ О ВИРУСНОСТИ КОНТЕНТА, НАРУШАЮЩЕГО ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ

К.В. Симонов, Д.М. Коваленко, О.А. Остапенко, В.В. Сафронова, К.В. Сибирко

В контексте обеспечения информационной безопасности рассматривается особый вид контента, вирусность которого побуждает интернет-пользователей знакомиться с его содержанием и распространять его в кибернетическом пространстве. Конструктивная привлекательность такого контента, зависящая от квалификации и изобретательности генерирующего его злоумышленника, открывает широкие перспективы для масштабного внедрения психологических и компьютерных вирусов, где сеть выступает как средство доставки. В работе анализируется традиционная идентификация вирусного контента, его свойство виральности, а также известные разновидности такого контента. При этом далее предполагается некоторое обобщение вирусной сущности контента в контексте обеспечения информационной безопасности интернет-пользователей. В целях развития научных исследований в области противодействия вирусным контентам предлагаются таблицы, формализующие этот процесс как в части понятийного аппарата, так и в отношении структуры решаемых задач.

Ключевые слова: интернет-пользователь, вирусный контент, виральность.