МЕТОДИКА ОЦЕНКИ СТОИМОСТИ ИНФОРМАЦИОННОГО РЕСУРСА

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

В статье на основании анализа руководящих документов ФСТЭК России предложена методика расчета количественной оценки стоимости информационного ресурса в денежном эквиваленте. В качестве базовой величины применена стоимость отдельного бизнес-процесса компании или организации. Методика позволяет рассчитать базовую и полную стоимость информационного ресурса как на отдельных шагах бизнес-процесса, так и в целом в рамках бизнес-процессов, используемых в организации или компании. Показана возможность применения методики при анализе рисков информационной безопасности в современных информационных системах, а также возможность расчетов стоимости для каждого из свойств информационного ресурса, таких как конфиденциальность, целостность или доступность.

Ключевые слова: информационный ресурс, информационная безопасность, методика, риски, расчет стоимости, инфраструктура как код.

ТЕРРИТОРИАЛЬНО-ДИНАМИЧЕСКИЕ МОДЕЛИ МАНИПУЛЯТИВНЫХ ВОЗДЕЙСТВИЙ В СОЦИАЛЬНЫХ СЕТЯХ

В.А. Минаев

В статье показано, что территориальные и динамические аспекты распространения информации в социальных сетях (СС), а следовательно, и манипулятивных воздействий (МВ) на население тесно связаны. Осуществлен детальный обзор факторов и моделей МВ в СС, особое внимание уделено динамическим моделям диффузии инноваций, дающим возможность обосновывать целенаправленное управление МВ. Методологическим инструментарием реализации таких моделей является подход, теоретически обоснованный и практически реализованный в своих работах Дж. Форрестером. Показана эволюция моделей инфицирования SIR до ее современной версии SEIRS, позволившая автору обосновать и реализовать целый ряд модификаций динамических моделей. Модификации модели были применены в сфере здравоохранения для изучения и прогнозирования заболеваний в области венерологии, дерматологии, психогенных депрессий. Моделирование латентного состояния в динамике преступного поведения позволило более качественно и точно решать задачи криминологического анализа и прогнозирования преступности, управления кадровыми ресурсами правоохранительных органов. В настоящее время модели применяются для исследования манипулятивных воздействий в СС, включая информационный терроризм и экстремизм. Кроме того, построены модели информационного противоборства с негативными воздействиями в СС. В качестве важных результатов, полученных в статье, представляются аналитические зависимости времени достижения максимума “зараженных” МВ в латентном состоянии, а также времени достижения 95% “зараженных” МВ в различных населенных пунктах. Перспективный практический результат связан с кластеризацией регионов Российской Федерации на однородные по распространению информации территории.

Ключевые слова: территориально-динамические аспекты распространения информации, манипулятивное воздействие, социальная сеть, инфицирование, информационное противоборство, кластерный анализ.

О ВЫБОРЕ ПАРАМЕТРОВ АВТОМАТНЫХ МОДЕЛЕЙ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ ОБЪЕКТОВ

А.Ю. Максимовский

В предыдущих работах 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 (регистры сдвига или их обобщения, обладающие необходимыми

свойствами для целей осуществления мониторинга информационной безопасности сетевых объектов) и ассоциированных с ними комбинаторных объектов. В настоящей работе путем изучения свойств групп рассматриваемых автоматных моделей предложены варианты расширения классов и оптимизации параметров автоматных моделей мониторинга информационной безопасности объектов сетевой инфраструктуры, основанные на контроле алгебраических и комбинаторных соотношений входных и выходных последовательностей указанных объектов.

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

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ (CPS)

П.Ю. Филяк, А.А. Изъюров, Д.А. Пажинцев, И.А. Тырин

Рассматривается вопрос оценки информационной безопасности киберфизических систем - cyber-physical system (CPS). В частности, сэмулированной системы, на базе смартфона Android, адекватно отражающей сущность и свойства CPS. Поведение и защищенность оценивалась в условиях сертифицированной лаборатории, позволяющей достоверно оценивать защищенность, свойства и поведение киберфизической системы в условиях преднамеренного воздействия электромагнитного и (или) другой физической природы.

Ключевые слова: киберфизические системы - cyber-physical system (CPS), электромагнитное воздействие, воздействие другой физической природы, защищенность, информационная безопасность, электромагнитное поле, физические поля, Bluetooth, Wi-Fi, IoT.

МЕТОДИКА ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ ПРИ ФУНКЦИОНИРОВАНИИ ПРОГРАММНЫХ СРЕДСТВ, ФОРМИРУЮЩИХ ТЕХНИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПРОГРАММНО УПРАВЛЯЕМЫХ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

В.И. Белоножкин, Ю.А. Дергачев, А.С. Турчин, А.В. Бабурин, А.С. Пахомова

В статье приводится методика оценки и регулирования рисков при функционировании вредоносных программных средств, формирующих технический канал утечки информации за счет программно-управляемых узкополосных ПЭМИ интерфейсов СВТ. Проведен анализ характеристик существующих на данный момент специальных программных средств, на основе которых могут создаваться программные закладки, организующие передачу конфиденциальных данных в радиоэфир. В ходе проведения оценки рисков были получены наиболее полные формулы, учитывающие основные факторы, позволяющие организовать утечку. При рассмотрении способов снижения риска была предложена схема формирования комплекса защитных мер. При рассмотрении существующих на данный момент средств и способов защиты информации от утечки по рассматриваемому каналу были описаны недостатки каждого из них. В рамках данной работы были получены выражения для нахождения меры риска – величины, показывающей степень значимости возникающего ущерба. Была построена матрица последствий и вероятностей, на основе которой предложены дополнительные организационные мероприятия, зависящие от степени воздействия риска. Была предложена формула для оценки эффективности внедряемых средств защиты, учитывающая такие факторы, как величина снижения риска от работы защиты и оценочные показатели принимаемого перечня издержек, полученные на основании экспертного мнения.

Ключевые слова: риск-анализ; технический канал утечки информации, создаваемый за счет программно-управляемых ПЭМИ (ТКУИ за счет ПУ ПЭМИ); программно-определяемое радио (SDR); интерфейс СВТ.

ИНСТРУМЕНТАРИЙ ДЛЯ АНАЛИЗА ИНТЕРНЕТ-РЕСУРСОВ В УСЛОВИЯХ РАСПРОСТРАНЕНИЯ ВИРУСНОГО КОНТЕНТА: СТРУКТУРА И ФУНКЦИОНАЛ МОНИТОРИНГА

Н.Г. Титов, А.Р. Кириллов, А.Г. Остапенко, А.В. Паринов, М.Е. Волкова

В статье предложен алгоритм работы системы мониторинга публичного Интернет-пространства, вне социальных сетей, на предмет выявления контентов с заданными свойствами. Рассматривается класс контентов, распространение которых в Интернет-пространстве может привести к негативным последствиям. Описана структура и функционал такой системы мониторинга. На основе этого реализовано специализированное программное обеспечение, показаны примеры и возможности его работы. Обоснован потенциал этой системы и предложены пути дальнейшего развития полученного программного обеспечения для мониторинга.

Ключевые слова: Интернет-пространство, системы мониторинга, сканирование ресурсов, контент.

ВЕКТОРНАЯ ОЦЕНКА ОПАСНОСТИ РАСПРОСТРАНЕНИЯ ВИРУСНЫХ КОНТЕНТОВ НА ОСНОВЕ СРЕДНЕСУТОЧНОЙ РЕАКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-РЕСУРСОВ

Ю. Штефанович, Е.А. Шварцкопф, В.В. Манмарева, Д.В. Манмарев, И.А. Боков

Представленная вниманию читателя работа по большему счету относится к серии тех публикаций, которые ищут в открытом доступе дополнительные информационные резервы для более глубокой аналитики, где приходится добывать актуальные данные как о ресурсах, так и циркулирующих в них контентах, особенно при разрешении проблемы оперативного (раннего) обнаружения и анализа резонансного контента. Эта проблемная операция должна обращаться к необходимым и достаточным по содержанию и объему информационным источникам, которые администратор сети (по прихоти и/или умыслу) не скроет от внешнего пользователя в одночасье. В этой связи авторы работы сочли уместным «добывать» характеристики из «афиши» ресурсов, т.е. из периодической статистики администрации сети (суточной, недельной, месячной) в отношении эмоционально-личностной реакции ее пользователей на контенты в рамках анализируемого ресурса (закрытие такой информации будет антирекламой для онлайн-сообщества).

Ключевые слова: интернет-ресурс, среднесуточные метрики, вектор, модуль.

ОЦЕНКА ЗАЩИЩЕННОСТИ UNIX-ПОДОБНЫХ ОПЕРАЦИОННЫХ СИСТЕМ ОТ ПРОГРАММНЫХ ЗАКЛАДОК И ВИРУСНЫХ ВОЗДЕЙСТВИЙ

Н.Н. Толстых, О.В. Поздышева, Е.С. Золотарева, А.В. Веденеев, В.И. Борисов

Цель исследования состоит в построении модельного представления процессов информационного взаимодействия и исследовании на основе этого особенностей внедрения вредоносного программного обеспечения в наиболее важные элементы операционной системы. В работе предлагается анализ и оценка защиты рассматриваемых операционных систем от информационных воздействий, возможность их внедрения и дальнейшего противодействия данным угрозам. Разработанное модельное представление функционирования компьютерных устройств учитывает искажения частной и общей целевой функций обрамляющих или конечных устройств в операционных средах семейства Unix, в условиях информационного воздействия на них. Созданное методическое и программное обеспечение, в отличие от аналогов, позволяет проводить оценку защищенности функционирования типовых операционных систем линейки Unix при информационных воздействиях в условиях неопределенности. В отличие от аналогичного инструментария, созданное прикладное программное обеспечение позволяет

эффективно обнаруживать операционные воздействия с учетом особенностей операционных систем Unix.

Ключевые слова: Unix, информационное воздействие, вирусы, программные закладки, телекоммуникационные сети связи и управления, операционные системы.

РИСК-РАНЖИРОВАНИЕ ОБЩЕДОСТУПНЫХ ИНТЕРНЕТ-РЕСУРСОВ НА ОСНОВЕ СРЕДНЕСУТОЧНЫХ ИЗМЕРЕНИЙ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ ВОСПРИЯТИЯ ИХ ПОЛЬЗОВАТЕЛЯМИ ВБРАСЫВАЕМЫХ КОНТЕНТОВ

Е. Ружицкий, Е.А. Шварцкопф, В.В. Манмарева, Д.В. Манмарев, С.В. Лихобабин

Предлагается в риск-анализе рассматриваемых интернет-ресурсов опираться на среднесуточную статистику реакции их пользователей на циркулирующие в них контенты. В этой связи вводятся определения параметров: степень вирусности контентов ресурса, степень генерационной активности пользователей ресурса, степень общей активности пользователей ресурса, степень вовлеченности пользователей ресурса и другие метрики. В качестве примера по предложенным метрикам были проанализированы онлайн-сообщества одного из регионов России, и из среднесуточного количества реакций удалось получить вышеуказанные степени. Далее на базе степени вовлеченности и доли региональных пользователей оценен риск успешного распространения негативных контентов в каждом из вышеупомянутых ресурсов, а также осуществлено ранжирование ресурсов по этому параметру. Предлагаемый подход в упорядочивании ресурсов будет полезен для объемного их мониторинга, когда приходится делать репрезентативную выборку.

Ключевые слова: интернет-ресурс, информационные процессы, среднесуточные метрики, риск.

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ СВЯЗИ И УПРАВЛЕНИЯ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, Я.М. Каценко, А.А. Болгов, В.В. Сафронова, К.В. Сибирко

Предлагается методика прогнозной оценки рисков нарушения безопасности, основанная на применении аппарата нечеткой логики. Проводится прогнозирование рисков на начальном этапе с помощью экспертов, которые оценивают входные параметры, с последующей обработкой с помощью предложенной иерархической методики применения систем нечеткого вывода, что позволяет уменьшить влияние субъективных оценок экспертов на исследуемый объект. Получены численные оценки риска, несмотря на качественный характер экспертных оценок входных параметров. Предложенная методика реализована с помощью имитационного программного комплекса и проведена проверка адекватности полученных результатов с помощью критерия Манна-Уитни. Представлена методика регулирования рисков, основанная на получении рекомендаций из публичных источников – реестров уязвимостей, а также зарубежных нормативно-правовых документов. Представлен программный инструментарий, позволяющий оперативно производить поиск по заданному признаку.

Ключевые слова: интернет вещей, сеть, риск, прогноз, экспертные оценки, нормативная документация, нечеткие множества.

МЕТОД АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ СТЕПЕНИ ОСНАЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ СРЕДСТВАМИ ФИЗИЧЕСКОЙ ЗАЩИТЫ

Е.В. Бурькова

Физическая защита объектов информатизации является важной частью комплексной системы безопасности. Процесс оценки степени оснащенности объекта информатизации средствами физической защиты является трудоемкой и ответственной задачей. Рассмотрены существующие подходы к формализации задачи оценки степени оснащенности объекта средствами физической защиты: экспертный, на основе вычисления вероятности исхода боестолкновения нарушителя и сил реагирования, лингвистический. В статье представлены функциональная и формализованная модели оценки степени оснащенности объекта средствами физической защиты. Показаны результаты программной реализации предлагаемого метода автоматизированной оценки степени оснащенности объекта информатизации средствами физической защиты с целью выявления наименее защищенных активов объекта и дальнейшей выработки рекомендаций по совершенствованию системы физической защиты.

Ключевые слова: степень оснащенности, формализованная модель, средства физической защиты, актуальные угрозы безопасности.

ТЕМАТИЧЕСКАЯ КЛАССИФИКАЦИЯ ИНТЕРНЕТ-РЕСУРСОВ НА ОСНОВЕ ВЕКТОРНОЙ ИЛЛЮСТРАЦИИ ПО ГРУППАМ ПОТЕНЦИАЛЬНО ОПАСНЫХ КОНТЕНТОВ

Е. Ружицикий, Е.А. Шварцкопф, В.В. Манмарева, Д.В. Манмарев, А.О. Ткаченко

В целях наглядной визуализации информационного процесса тематической классификации интернет-ресурса предлагается векторный подход для оценки тематик его контентов. В частности, по обобщенной классификации противоправных контентов предлагается сконцентрировать в определенных квадрантах тематической плоскости векторы контентов заданного качества. Для количественной оценки модуля этих векторов предложено отношение количества контентов заданного качества к общему количеству контентов ресурса, скажем, за неделю. Таким образом можно получить тематические портреты террористических сайтов, «групп смерти», мошеннических ресурсов и т.п. Далее предлагаются метрики оценки модулей вышеуказанных векторов на основе еженедельных метрик реактивности пользователей ресурса. При этом предлагаются количественные оценки для превосходства (доминирования) той или иной тематики в рамках исследуемого интернет-ресурса.

Ключевые слова: интернет-ресурс, контент, тематика, вектор, модуль.

ИСПОЛЬЗОВАНИЕ МЕНТАЛЬНЫХ КАРТ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, С.В. Королев, Н.В. Тебеньков, В.А. Мальцева, И.С. Перевезенцев, И.А. Захаренков, Г.А. Чекина

В статье рассматривается применение ментальных карт для решения проблем обеспечения информационной безопасности, для решения которых в условиях современности требуется использование новых подходов и методов. В этой связи целесообразно использовать такой инструмент, как ментальные карты. С точки зрения концепции развития искусственного интеллекта в РФ использование ментальных карт является промежуточным этапом при переходе к использованию более серьезных инструментов.

Ключевые слова: анализ, графическая визуализация, информационная безопасность, карта мыслей, когнитивные карты, ментальные карты, процесс мышления.

ПРИМЕНЕНИЕ СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТКС

П.Ю. Филяк, А.Н. Ермолин, Д.С. Семяшкина, М.А. Корецкий, И.С. Колобов

В статье рассматриваются организационно-технологический и инженерно-технический методы защиты информации и их инструменты – средства защиты информации (СЗИ) для обеспечения информационной безопасности информационно-телекоммуникационной сети (ИТКС), к каковым можно отнести любую корпоративную информационную систему (КИС). При всей кажущейся на первый взгляд простоте данный тип задач нельзя никоим образом отнести к тривиальным, поскольку, с одной стороны, применяемые СЗИ представляют собой сертифицированные решения с совершенно определенными диапазонами технических и технологических параметров, что требует весьма непростой и точной настройки и адаптации, с другой стороны, комплексная защита информации требует применения различных СЗИ, отличающихся не только своими характеристиками, но производителями, что автоматически генерирует целый спектр дополнительных задач, а зачастую даже проблем.

Ключевые слова: информация, защита информации, информационно-телекоммуникационная сеть (ИТКС), средства защиты информации (СЗИ), информационная безопасность.