РИСК-АНАЛИЗ И ПРОГНОЗИРОВАНИЕ ЧАСТОТЫ И УЩЕРБНОСТИ КОМПЬЮТЕРНЫХ АТАК

А.Л. Сердечный, А.С. Маликова, А.Г. Остапенко, М.Е. Волкова, Д.А. Нархов, А.Н. Бартенев

Рассматривается статистика частоты и ущербности компьютерных атак для различных их разновидностей. Предлагается соответствующее методическое обеспечение, и приводятся результаты его практического применения для прогнозирования киберпреступности по отдельным его видам и типам. Приводится аналитика ожидаемых перспектив и трендов популярности наиболее опасных видов атак по странам и в мировом масштабе. С учетом осуществленного прогнозирования выработаны рекомендации по совершенствованию системы противодействия компьютерным атакам.

Ключевые слова: риск-анализ, компьютерная атака, нормированный риск, усредненный риск, статистика.

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

А.Л. Сердечный, Г.В. Сторожев, М.А. Тарелкин, А.С. Пахомова

В статье проведен анализ нормативных актов по организации обработки и защите В настоящей статье представлены результаты моделирования способов реализации компьютерных атак на мобильные устройства. Актуальность данной статьи обусловлена отсутствием наработок по формированию методического обеспечения, касающегося моделирования способов реализации компьютерных атак на мобильные устройства, учитывающего их специфику. Предложенные модели способов предназначены для формирования методического обеспечения расчета рисков и выявления оценки защищенности таких систем от актуальных сценариев реализации угроз безопасности информации, которое даёт возможность обоснованного выбора мер защиты. Построение моделей способов реализации компьютерных атак осуществлялось с использованием аппарата сетей Петри на основании сведений, содержащихся в базе данных MITRE ATT&CK. Разработанные модели взаимосвязаны по условиям и последствиям реализации основных технических приёмов, определённых в базе данных ATT&CK и актуальных для мобильных устройств (условия и последствия моделируются позициями сети Петри, а сами технические приёмы – переходами сети Петри). Также в статье затрагиваются вопросы автоматизации и совместной разработки подобных моделей. Проводится сравнительный анализ различных форм представления участков моделируемой сети Петри в контексте удобства процесса её разработки

Ключевые слова: сети Петри, ATT&CK, атаки на мобильные устройства, анализ, визуализация.

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ ПОДГОТОВКИ КОМПЬЮТЕРНЫХ АТАК В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.Л. Сердечный, Н.С. Пустовалов, М.А. Тарелкин, А.Е. Дешина

Цель проведённых исследований заключалась в формализации действий нарушителя, совершаемых в ходе подготовки компьютерной атаки как основного этапа, на котором можно оказать противодействие нарушителю до того, как защищаемой системе будет нанесён ущерб. В настоящей статье представлены результаты разработки модели сети Петри для этапа подготовки к компьютерной атаке в распределенных компьютерных системах. Модель учитывает причинно-следственные связи между действиями нарушителя, а также условиями и последствиями реализации таких действий. Наличие таких связей позволяет определять сценарии подготовки компьютерных атак в зависимости от структурных и функциональных особенностей объекта защиты и модели нарушителя. Разработанная модель может быть использована в качестве исходных данных при моделировании угроз безопасности информации в части определения способов, используемых нарушителем при выборе объекта атаки, а также в ходе получения необходимых ресурсов для её совершения. Также в настоящей статье продемонстрирована возможность моделирования мер защиты, затрудняющих реализацию сценария к атаке.

Ключевые слова: сеть Петри, ATT&CK, подготовка компьютерной атаки, моделирование.

СЕТЕВАЯ ВИРУСОЛОГИЯ: ПРОГНОЗИРОВАНИЕ РАЗВИТИЯ ДВУВИРУСНЫХ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ В СЕТЯХ

А.Г. Остапенко, Е.В. Зарочинцев, О.А. Остапенко, К.В. Сибирко, В.В. Сафронова, П.Д. Федоров

Целью исследований является повышение защищённости распределенных компьютерных сетей за счет формализации поливирусных эпидемических процессов в них на основе специально созданного методического поливирусного обеспечения оценки и регулирования рисков. В работе продемонстрированы поливирусные модели, позволяющие моделировать поливирусное воздействие на компьютерную сеть. При помощи представленных моделей было произведено моделирование поливирусного воздействия на сетевую структуру. Полученные результаты могут быть использованы исследователями в области моделирования эпидемических процессов, данные модели позволят более точно и качественно оценивать протекание поливирусных эпидемических процессов в распределённых компьютерных сетях, а также специалистами по защите информации при разработке мер противодействия распространения компьютерных вирусов и реализовать задел к рассмотрению скоростных и качественных особенностей протекания поливирусных эпидемических процессов в компьютерных сетях.

Ключевые слова: поливирусное воздействие, эпидемический процесс, модель.

АНАЛИЗ ПРОТОКОЛОВ ЗАЩИТЫ И ОЦЕНКА РИСКА ИХ ПРИМЕНЕНИЯ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.С. Тулинов, А.А. Болгов, В.К. Власов

В данной статье предлагается методика повышения защищенности сетей и конечных устройств интернета вещей от атак, направленных на нарушение конфиденциальности информации и процедуры аутентификации, за счет внедрения новых несертифицированных протоколов обеспечения безопасности и создания методического обеспечения для оценки рисков успешной реализации атак. В работе были смоделированы и проанализированы протоколы безопасности технологии интернета вещей с помощью специализированного инструмента моделирования. При использовании результатов моделирования для всех протоколов, представленных в данной работе, был посчитан риск успешной реализации атак, направленных на нарушение конфиденциальности информации и процедуры аутентификации. На основе полученных значений было выполнено сравнение протоколов безопасности. Результаты проделанной работы позволят упростить разработку и внедрение новых протоколов безопасности для технологии интернета вещей.

Ключевые слова: интернет вещей, протокол, моделирование, ущерб, риск, атака.

ЦЕЛЕВАЯ КОМПЛЕКСНОСТЬ ПРОГРАММЫ ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Л.В. Астахова, С.А. Бесчастнов

Повышение осведомленности сотрудников организации об информационной безопасности занимает устойчивое место в числе объектов исследования науки и практики, что обусловлено объективными факторами. Результаты исследований показывают, что в организациях присутствуют проблемные области управления информационной безопасностью, связанные с отсутствием целенаправленно применяемой методологии обучения и профессионального развития пользователей информационных систем. Это выражается в росте числа утечек защищаемой информации, спровоцированных внутренними пользователями. Для решения этой проблемы в статье обоснована сущность принципа целевой комплексности программы повышения осведомленности сотрудников об информационной безопасности организации, его доминирующая роль в процессе проектирования структуры и содержания программы. Охарактеризовано разработанное на основе этого принципа программное средство для повышения осведомленности сотрудников, его технические параметры, функциональные возможности и отличия от других продуктов.

Ключевые слова: целевая комплексность, повышение осведомленности, программа, сотрудник, информационная безопасность.

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ФУНКЦИОНИРОВАНИЯ SOC-ЦЕНТРА ПРЕДПРИЯТИЯ В УСЛОВИЯХ МАСШТАБНЫХ КОМПЬЮТЕРНЫХ АТАК

В.А. Минаев, Е.С. Поликарпов

Обсуждаются структура современных центров мониторинга информационной безопасности (ЦМИБ) и схема прохождения сообщений через блок SIEM (Security Information and Event Management). Дано ограничение на время обработки сообщения о событиях в SIEM. Изучены результаты некоторых имитационных экспериментов с управлением кадровыми ресурсами SOC-Центра. Показано, что для оптимизации управления ресурсами центров обеспечения информационной безопасности современных предприятий эффективно применимы методы дискретно-событийного моделирования. Разработанная авторами дискретно-событийная модель SOC-центра позволяет решать задачи управления и оптимизации кадрового ресурса, прогнозирования и анализа поведения центра при различных штатных и внештатных ситуациях.

Выбранное в качестве среды имитационного моделирования программное обеспечение Anylogic позволяет воспроизводить различные сценарии с помощью дискретно-событийных моделей, производить интерпретацию результатов моделирования и управлять факторным комплексом моделей во время их работы, проводить различные виды имитационных экспериментов, в том числе – по вариации параметров моделей, оптимизации и многое другое.

Эксперименты подтвердили устойчивость и адекватность математической модели оптимизации управления кадровыми ресурсами. При проведении исследований дискретно-событийной модели SOC-центра показано, что организация борьбы с компьютерными атаками осуществляется эффективнее при оптимальном распределении кадровых ресурсов. В ходе эксперимента по организации целенаправленной компьютерной атаки выявлено, что модель с оптимальным распределением кадрового ресурса устойчива к атакам различного масштаба, включая массовые.

Ключевые слова: информационная безопасность, предприятие, мониторинг, компьютерная атака, имитационное моделирование, кадровое обеспечение SOC-центра, оптимизация.

МЕТОДИКА ОПТИМИЗАЦИИ ЭЛЕМЕНТОВ ИНТЕГРАЛЬНО-ОПТИЧЕСКОГО МОДУЛЯ АУТЕНТИФИКАЦИИ

О.А. Кулиш

В ходе информационного обмена между локальными вычислительными сетями пользователей передаваемая информация проходит через не защищенную сеть провайдера связи. Отсутствие аутентификации коммутаторов позволяет злоумышленникам осуществлять сетевые атаки на коммутаторы второго уровня модели OSI. Для устранения проблемы аутентификации коммутационного оборудования канального уровня можно использовать модуль аутентификации, встроенный в коммутатор. В работе приведена схема интегрально-оптического интерферометра для устройства управления оптическим излучением модуля аутентификации. Так как для передачи кода аутентификации применяется ослабленное лазерное излучение, то актуальным является расчет потерь оптического сигнала в интерферометре. Высокие потери оптического излучения могут происходить во внутреннем двойном изгибе спирали и во входном и выходном разветвителях интерферометра. Разработана методика оптимизации этих элементов интерферометра для уменьшения потерь оптического сигнала. Методика основана на методе распространяющегося пучка, методе эффективного показателя преломления и конечно-элементном анализе. На основе разработанной методики можно оценить оптимальное смещение волноводов в точке перегиба внутреннего S-изгиба спирали, геометрические параметры входного и выходного разветвителей.

Ключевые слова: оптическая связь, аутентификация, коммутаторы, интегральная оптика, интерферометр, численные методы, энергетические потери.

ПРИМЕНЕНИЕ МЕХАНИЗМА МНОГОУРОВНЕВОЙ СПРАВЕДЛИВОЙ ОЧЕРЕДИ ДЛЯ СНИЖЕНИЯ УЩЕРБА ОТ АТАК ОТКАЗА В ОБСЛУЖИВАНИИ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

М.Ю. Рытов, Р.Ю. Калашников, А.А. Горелов

Концепция программно-конфигурируемых сетей (SDN) стремительно набирает популярность в управлении сетевой инфраструктурой центров обработки данных и операторов связи. К её ключевым функциям относятся мониторинг, детальное управление, гибкость и масштабируемость. Но вместе с тем, централизованное управление SDN делает его уязвимым для различных типов атак, таких как спуфинг и отказ в обслуживании (DoS). DoS-атаки оказывают наиболее серьезное воздействие, поскольку они снижают производительность сети из-за перегрузки ее различных компонентов, то есть контроллера, коммутатора и канала управления. Существующие подходы справляются с DoS-атаками в SDN либо путем отбрасывания вредоносных пакетов, либо путем объединения правил потока, что приводит к потерям легитимного трафика. Для уменьшения последствий DoS-атак в этой статье предлагается использование механизма многоуровневой справедливой очереди, который обеспечивает совместное использование ресурсов контроллера с несколькими уровнями очередей, которые могут динамически расширяться и агрегироваться в зависимости от загруженности сети. Предлагаемый подход оценивается путем сравнения его с базовым контроллером SDN. Результаты моделирования показывают, что предлагаемый подход увеличивает производительность SDN с точки зрения использования пропускной способности канала управления.

Ключевые слова: сетевая безопасность, отказ в обслуживании, программно-конфигурируемые сети.

АНАЛИЗ БЕЗОПАСНОСТИ ЗАЩИЩЕННЫХ И АНОНИМНЫХ БРАУЗЕРОВ

Ю.Ю. Громов, О.В. Трубиенко, П.И. Карасев, К.А. Желобенко

Индустрия браузеров существует в основном за счет косвенных источников финансирования, поэтому создатели браузеров должны заботиться о привлекательности предлагаемого продукта. При выборе браузера пользователь руководствуется соображениями красоты, удобства и скорости работы. Большинство пользователей в современном мире не являются технически подготовленными, это обычные люди, которые подбирают товары в магазинах или общаются в соцсетях и т. п. Они имеют смутные представления об информационной безопасности и часто пренебрегают ею либо, наоборот, начинают бояться вмешательства в частную жизнь и не знают, как себя обезопасить или как проверить ее обеспечение. Поэтому основная ответственность обеспечения информационной безопасности лежит на создателях браузера и зависит от их добросовестности и компетенции. Одна из задач специалистов по информационной безопасности – помогать улучшать сервисы с точки зрения их безопасности. С этой целью в работе проведен анализ безопасности четырех браузеров, которые были изначально представлены как браузеры для безопасного и анонимного пользования. Задача обзора и анализа заключается в определении наиболее безопасного и конфиденциального инструмента для веб-серфинга, а также выявления содержания в этих браузерах вредоносных кодов.

Ключевые слова: безопасные браузеры, анонимность, конфиденциальность в сети.

КОЛИЧЕСТВЕННАЯ ОЦЕНКА ДЕСТРУКТИВНОСТИ БОЛЬШИХ ТЕКСТОВЫХ МАССИВОВ В СОЦИАЛЬНЫХ МЕДИА

В.А. Минаев, А.В. Симонов

Цель исследования состоит в разработке методики, позволяющей выявлять деструктивность больших текстовых массивов в социальных медиа. Проведен анализ существующих подходов к определению деструктивного характера текстовых данных, дано описание их преимуществ и недостатков. Описан метод определения деструктивности текста с использованием векторных представлений слов. Рассмотрено формирования векторных представлений слов и оценена возможность их применения при решении задач идентификации текстового контента. Обосновано применение алгоритмов Word2vec и FastText. Предложены ключевые слова и выражения векторных представлений слов, определяющих три класса текстов: реабилитация нацизма, радикальный ислам, антисемитизм. Реализованы модели выявления деструктивности контента больших текстовых массивов с использованием нейтральных новостных корпусов текстов и текстов, содержащих возможный деструктивный контент. Произведена интерпретация результатов анализа текстовых массивов и обоснована Word2vec как наиболее подходящая модель векторного представления слов. Сделан вывод о направлениях использования полученных результатов в аналитической деятельности государственных органов, общественных организаций и социальных медиа для выявления противоправного контента.

Ключевые слова: информационная безопасность, социальные медиа, деструктивный контент, мониторинг, идентификация.

КАРТОГРАФИЧЕСКИЕ МОДЕЛИ ПРОЦЕССОВ ДИФФУЗИИ ВРЕДОНОСОВ В СЕТЕВОМ КИБЕРПРОСТРАНСТВЕ

А.Г. Остапенко, А.Л. Сердечный, А.А. Остапенко, С.С. Куликов

Рассматривается весьма актуальная проблема моделирования процесса диффузии вредоносных кодов и деструктивных контентов в киберпространстве, которое в современных условиях носит все более выраженный сетевой характер. В отличии от ранее широко используемых аналоговых и даже развивающих их дискретных эпидемических моделей, в настоящей работе учитываются статический (накопленную информацию) и динамический (информационный трафик) ресурсы узлов и ветвей сети. Наряду с этим принимается во внимание дозировка вредоноса, внедряемого в сеть для нарушения её работоспособности. Все это позволяет осуществить сетевое картографирование эпидемического процесса, порождаемого в результате диффузии вредоносной инъекции. Предлагаемая модель открывает новую страницу в описании информационных эпидемий (и не только) во взвешенных сетях, где предлагаемая авторами формализация масштабирует изображаемые размеры узлов и ветвей модели в соответствии со значениями ресурсов или потенциалов её элементов. Фактически получается граф (карта) исследуемого сетевого ландшафта, в котором циркулирует информация. В случае внедрения вредоноса компоненты карты окрашиваются с учетом дозировки его присутствия в них, где топологической основой выступают “звезды” сети. Для этого авторами предлагаются соответствующие аналитические выражения.

Ключевые слова: картографические модели, киберпространство, вредоносы, алгоритмы.

НАУЧНО-ТЕХНИЧЕСКИЕ РЕЗУЛЬТАТЫ И ПЕРСПЕКТИВЫ РЕАЛИЗАЦИИ ПРОЕКТА «БЕЗОПАСНЫЙ ИНТЕРНЕТ»

А.Г. Остапенко, И.А. Боков, А.А. Остапенко, Н.М. Лантюхов, Т.Ю. Мирошниченко, С.В. Лихобабин, С.Д. Трубицын

Рассматриваются цели, задачи и текущие результаты проекта «Безопасный Интернет». В этой связи формулируется мотивация создания проекта в условиях геополитической и цифровой трансформации глобального информационного общества. Кроме того, иллюстрируются основные результаты, полученные в ходе реализации проекта. При этом, авторами (с учетом футурологических прогнозов) дается краткий обзор вариантов развития политической и цифровой трансформации, а также – предлагаются горизонты развития предметной области настоящей работы и проекта «Безопасный Интернет». Фактически демонстрируются текущие достижения проекта и намечаются пути его совершенствования в современных условиях состояния и динамики глобального информационного пространства.

Ключевые слова: контент, цифровая трансформация, пандемия.