DOI 10.36622/VSTU.2021.24.2.001
УДК 004.056

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.

RISK ANALYSIS AND FORECASTING TRENDS IN CRIMINAL TELECOMMUNICATIONS ATTACKS

A.L. Serdechnyy, A.S. Malikova, A.G. Ostapenko, M.E. Volkova, D.A. Narkhov, A.N. Bartenev

Statistics of frequency and damage of telecommunication attacks for their various varieties are considered. The corresponding methodological support is proposed, and the results of its practical application for predicting cybercrime by its individual types and types are presented. An analysis of the expected prospects and trends of popularity of the most dangerous types of crimes by countries and on a global scale is given. Taking into account the carried out forecasting, recommendations were made to improve the system of countering cybercrime.

Keywords: risk-analysis, telecommunication attack, normalized risk, averaged risk, statistics.

DOI 10.36622/VSTU.2021.24.2.002
УДК 004.056

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.

MODELING, ANALYSIS, AND COUNTERACTION MEASURES FOR IMPLEMENTATION SCENARIOS OF INFORMATION SECURITY THREATS ON MOBILE DEVICES

A.L. Serdechnyy, G.V. Storozhev, M.A. Tarelkin, A.S. Pahomova

This article presents the results of modeling methods for implementing computer attacks on mobile devices. The relevance of this article is due to the lack of developments in the formation of methodological support for modeling methods for implementing computer attacks on mobile devices, taking into account their specifics. These models are intended for the formation of methodological support for calculating risks and identifying the assessment of the security of such systems from current scenarios of information security threats, which makes it possible to make an informed choice of security measures. The construction of models of ways to implement computer attacks was carried out using the device of Petri nets based on the information contained in the MITRE ATT&CK database. These models are interconnected by the conditions and consequences of the implementation of the main techniques defined in the ATT&CK database and relevant for mobile devices (conditions and consequences are modeled by the positions of the Petri net, and the techniques themselves are modeled by the transitions of the Petri net). In article also addresses the issues of automation and joint development of such models. A comparative analysis of various forms of representation of the sections of the simulated Petri net in the context of the convenience of its development process is carried out.

Keywords: Petri nets, ATT&CK, attacks on mobile devices, analysis, visualization.

DOI 10.36622/VSTU.2021.24.2.003
УДК 004.056

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.

MODELING, ANALYSIS AND COUNTERING THE SCENARIOS OF PREPARING COMPUTER ATTACKS IN DISTRIBUTED COMPUTER SYSTEMS

A.L. Serdechnyy, N.S. Pustovalov, M.A. Tarelkin, A.E. Deshina

The purpose of the research was to formalize the actions of the violator committed during the preparation of a computer attack as the main stage at which it is possible to counteract the violator before the protected system is damaged. This article presents the results of the development of a Petri net model for the preparation stage for a computer attack in distributed computer systems. The model takes into account the causal relationships between the actions of the violator, as well as the conditions and consequences of the implementation of such actions. The presence of such links allows you to determine the scenarios for preparing computer attacks, depending on the structural and functional features of the object of protection and the model of the intruder. The developed model can be used as a source data for modeling information security threats in terms of determining the methods used by the violator when choosing the object of the attack, as well as in the course of obtaining the necessary resources for its commission. This article also demonstrates the possibility of modeling security measures that make it difficult to implement a scenario for an attack.

Keywords: Petri net, ATT&CK, computer attack preparation, simulation.

DOI 10.36622/VSTU.2021.24.2.004
УДК 004.35

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.

NETWORK VIROLOGY: PREDICTION AND REGULATION OF MULTIVIRUS EPIDEMIC PROCESSES

A.G. Ostapenko, E.V. Zarochentsev, O.A. Ostapenko, K.V. Sibirko, V.V. Safronova, P.D. Fedorov

The purpose of the research is to increase the security of distributed computer networks by formalizing the multivirus epidemic processes in them on the basis of a specially created methodological multivirus support for risk assessment and management. The work demonstrates polyviral models that allow simulating a polyviral effect on a computer network. The presented models were used to simulate the polyviral effect on the network structure. The results obtained can be used by researchers in the field of modeling epidemic processes, these models will allow for a more accurate and high-quality assessment of the course of polyviral epidemic processes in distributed computer networks, as well as information security specialists in the development of measures to counter the spread of computer viruses, and features of the course of polyviral epidemic processes in computer networks.

Keywords: multivirus exposure, epidemic process, model.

DOI 10.36622/VSTU.2021.24.2.005
УДК 004.733

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.

ANALYSIS OF PROTECTION PROTOCOLS AND RISK ASSESSMENT OF THEIR USE IN INTERNET NETWORKS

S.A. Ermakov, A.S. Tulinov, A.A. Bolgov, V.K. Vlasov

This article proposes a method for improving the security of the networks and end devices of the Internet of Things from attacks aimed at violating the confidentiality of information and authentication procedures by introducing new uncertified security protocols and creating methodological support for assessing the risks of successful implementation of attacks. The security protocols of the Internet of Things technology were modeled and analyzed using a specialized modeling tool. When using the simulation results for all the protocols presented in this work, the risk of successful implementation of attacks aimed at violating the confidentiality of information and the authentication procedure was calculated. Based on the obtained values, a comparison of security protocols was performed. The results of this work will simplify the development and implementation of new security protocols for the Internet of Things technology.

Keywords: Internet of Things, protocol, modeling, damage, risk, attack.

DOI 10.36622/VSTU.2021.24.2.006
УДК 004.588

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.

TARGETED COMPREHENSION OF THE PROGRAM OF INCREASING AWARENESS OF EMPLOYEES ON INFORMATION SECURITY OF THE ORGANIZATION

L.V. Astakhova, S.A. Beschastnov

Raising the awareness of employees of the organization about information security takes a stable place among the objects of research in science and practice, which is due to objective factors. Research results show that organizations have problem areas of information security management associated with the lack of a purposefully applied methodology for training and professional development of information system users. This leads to an increasing number of information leaks through the fault of users. To solve this problem, the article substantiates the essence of the principle of the target complexity of the program for raising the awareness of employees about the information security of an organization, its dominant role in the process of designing the structure and content of the program. A software tool developed based on this principle for raising employee awareness, its technical parameters, functionality, and differences from other products is characterized.

Keywords: target complexity, awareness raising, program, employee, information security.

DOI 10.36622/VSTU.2021.24.2.007
УДК 004.056.53

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.

SIMULATION OF ENTERPRISE SOC-CENTER FUNCTIONING AT THE LARGE-SCALE COMPUTER ATTACKS

V. A. Minaev, E. S. Polikarpov

The structure of modern Information Security Monitoring Centers (ISMC) and the scheme of passing messages through the SIEM (Security Information and Event Management) block are discussed. The time limit for processing the event message in SIEM is given. The results of some simulation experiments with the human resources of the SOC-center are investigated. It is shown that the methods of discrete-event modeling are effectively applied to optimize the resource management of information security centers of modern enterprises. The discrete-event model of the SOC-center developed by the authors allows solving the problems of managing and optimizing the human resource, predicting and analyzing the behavior of the center in various regular and emergency situations.

The Anylogic software chosen as the simulation environment allows you to reproduce various scenarios using discrete-event models, interpret the simulation results and manage the factor complex of models during their operation, conduct various types of simulation experiments, including model parameter variations, optimization, and much more.

The experiments confirmed the stability and adequacy of the mathematical model for optimizing human resource management. When conducting studies of the discrete-event model of the SOC-center, it is shown that the organization of the fight against computer attacks is carried out more efficiently with an optimal distribution of human resources. During the experiment on the organization of a targeted computer attack, it was revealed that the model with the optimal distribution of human resources is resistant to attacks of various scales, including mass ones.

Keywords: information security, enterprise, monitoring, computer attack, simulation modeling, SOC center staffing, optimization.

DOI 10.36622/VSTU.2021.24.2.008
УДК 654.02

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.

METHOD OF OPTIMIZING ELEMENTS OF INTEGRATED OPTICAL AUTHENTICATION MODULE

O.A. Kulish

During information exchange between local computer networks of users, the transmitted information passes through an unprotected network of a communication provider. The lack of switch authentication allows attackers to carry out network attacks on Layer 2 switches of the OSI model. You can use the authentication module built into the switch to resolve the link layer switching equipment authentication problem. The work shows the integrated optical interferometer circuit for the optical radiation control device of the authentication module. Since attenuated laser light is used to transmit the authentication code, the calculation of optical signal losses in the interferometer is relevant. High losses of optical radiation can occur in the inner double bend of the spiral and in the input and output splitters of the interferometer. A technique has been developed to optimize these interferometer elements to reduce optical signal losses. The technique is based on the propagating beam method, the effective refractive index method, and finite element analysis. Based on the developed technique, the optimal displacement of waveguides at the inflection point of the internal S-bend of the spiral, the geometric parameters of the input and output splitters can be estimated.

Keywords: optical communication, authentication, switches, integrated optics, interferometer, numerical methods, energy losses.

DOI 10.36622/VSTU.2021.24.2.009
УДК 4.007

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.

APPLICATION OF MULTI-LEVEL FAIR QUEUE MECHANISM FOR MITIGATING DENIAL-OF-SERVICE ATTACKS ON SOFTWARE-DEFINED NETWORKS

M.Y. Rytov, R.Y. Kalashnikov, A.A. Gorelov

The concept of Software Defined Networking (SDN) is rapidly gaining popularity in the management of the network infrastructure of data centers and telecom operators. Its key functions include monitoring, granular control, flexibility and scalability. But at the same time, the centralized management of SDN makes it vulnerable to various types of attacks, such as spoofing and denial of service (DoS). DoS attacks have the most serious impact because they degrade network performance by overloading various components such as the controller, switch, and control channel. Existing approaches deal with SDN DoS attacks either by dropping malicious packets or by combining flow rules, which leads to the loss of legitimate traffic. To mitigate the impact of DoS attacks, this article proposes the use of a tiered fair queuing mechanism, which allows the sharing of controller resources with multiple queue tiers that can dynamically expand and aggregate based on network congestion. The proposed approach is evaluated by comparing it to a basic SDN controller. Simulation results show that the proposed approach increases SDN performance in terms of control channel bandwidth utilization.

Keywords: network security, denial of service, software defined networks.

DOI 10.36622/VSTU.2021.24.2.010
УДК 004.056

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.

SECURITY ANALYSIS OF PROTECTED AND ANONYMOUS BROWSERS

Y.Y. Gromov, O.V. Trubienko., P.I. Karasev, K.A. Gelobenko

The browser industry is largely driven by indirect funding, so browser makers should be concerned about the attractiveness of the product they offer. When choosing a browser, the user is guided by considerations of beauty, convenience and speed of work. Most users in the modern world are not technically trained, they are ordinary people who pick up products in stores or communicate on social networks, etc. They have a vague idea of information security, and often neglect it, or, on the contrary, begin to fear interference with their privacy and do not know how to protect themselves or how to check its provision. Therefore, the main responsibility for ensuring information security lies with the creators of the browser and depends on their integrity and competence. One of the tasks of information security professionals is to help improve services in terms of their security. To this end, the work carried out a security analysis of four browsers that were originally presented as browsers for safe and anonymous use. The task of the survey and analysis is to determine the most secure and confidential tool for web surfing, as well as to identify the content of malicious codes in these browsers.

Keywords: secure browsers, anonymity, online privacy.

DOI 10.36622/VSTU.2021.24.2.011
УДК 070.1:004.538

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.

QUANTIFICATION OF LARGE TEXT ARRAYS DESTRUCTIVENESS IN SOCIAL MEDIA

V.A. Minaev, A.V. Simonov

The aim of the study is to develop a method that allows us to identify the destructiveness of large text arrays in social media. The analysis of existing approaches to determining the destructive nature of text data is carried out, and their advantages and disadvantages are described. A method for determining the destructiveness of a text using vector representations of words is described. The formation of vector representations of words is considered and the possibility of their application in solving problems of identifying text content is evaluated. The application of the Word2vec and FastText algorithms is justified. Keywords and expressions of vector representations of words defining three classes of texts are proposed: rehabilitation of Nazism, radical Islam, and anti-Semitism. Models are implemented to identify the destructiveness of the content of large text arrays using neutral news text corpora and texts containing possible destructive content. The results of the analysis of text arrays are interpreted and Word2vec is justified as the most suitable model for the vector representation of words. The conclusion is made about the directions of using the obtained results in the analytical activities of state authorities, public organizations and social media to identify illegal content.

Keywords: information security, social media, destructive content, monitoring, identification.

DOI 10.36622/VSTU.2021.24.2.012
УДК 004.056

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.

CARTOGRAPHIC MODELS OF PEST DIFFUSION PROCESSES IN NETWORK CYBERSPACE

A.G. Ostapenko, A.L. Serdechnyy, A.A. Ostapenko, S.S. Kulikov

The article deals with a very relevant problem of modeling the process of diffusion of malicious codes and destructive content in cyberspace, which in modern conditions has an increasingly pronounced network character. In contrast to the previously widely used analog and even developing discrete epidemic models, this paper takes into account the static (accumulated information) and dynamic (information traffic) resources of nodes and branches of the network. Along with this, the dosage of the malware introduced into the network to disrupt its performance is taken into account. All this makes it possible to carry out network mapping of the epidemic process generated as a result of the diffusion of malicious injection. The proposed model opens a new page in the description of information epidemics (and not only) in weighted networks, where the formalization proposed by the authors scales the depicted sizes of nodes and branches of the model in accordance with the values of resources or potentials of its elements. In fact, a graph (map) of the network landscape under study is obtained, in which information circulates. In the case of the introduction of the malware, the map components are colored taking into account the dosage of its presence in them, where the topological basis is the “stars” of the network. For this purpose, the authors propose the corresponding analytical expressions.

Keywords: cartographic models, cyberspace, malware, algorithms.

DOI 10.36622/VSTU.2021.24.2.013
УДК 004.056

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.

SCIENTIFIC AND TECHNICAL RESULTS AND PROSPECTS OF THE "SECURE INTERNET" PROJECT IMPLEMENTATION

A. G. Ostapenko, I. A. Bokov, A. A. Ostapenko, N. M. Lantyukhov, T. Yu. Miroshnichenko, S. V. Likhobabin, S. D. Trubitsyn

The goals, objectives and current results of the "Secure Internet"project are considered. In this regard, the motivation for the creation of the project in the context of the geopolitical and digital transformation of the global information society is formulated. In addition, the main results obtained during the implementation of the project are illustrated. At the same time, the authors (taking into account futurological forecasts) give a brief overview of the options for the development of political and digital transformation, as well as suggest the development horizons of the subject area of this work and the project "Safe Internet". In fact, it demonstrates the current achievements of the project and outlines ways to improve it in the current conditions of the state and dynamics of the global information space.

Keywords: content, digital transformation, pandemic.