DOI 10.36622/VSTU.2023.4.26.001
УДК 004.056

ЦЕЛЕПОЛАГАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПО СОЗДАНИЮ ИНСТРУМЕНТАРИЯ АВТОМАТИЗИРОВАННОГО ВЫЯВЛЕНИЯ И РИСК-АНАЛИЗА ДЕСТРУКТИВНЫХ КОНТЕНТОВ, АФФИЛИРОВАННЫХ С ПЕРСОНАЛОМ КОРПОРАЦИЙ

А.Г. Остапенко, И.А. Боков, С.В. Лихобабин, Д.С. Ясенко, Е.Ю. Чапурин

Рассматриваются видео, аудио и графические контенты социальных сетей как фактор обеспечения информационной безопасности корпораций. Осуществляется целеполагание проектной деятельности по созданию автоматизированного инструментария выявления и риск-анализа вышеуказанных контентов, включая парсинг ресурсов соцсетей, селекцию собранных контентов по признакам деструктивности и их риск-анализ для выработки рекомендаций по разграничению доступа к корпоративной информации. Оценивается актуальность проектной деятельности, исследуются аналоги, предлагаются архитектура и алгоритмы создаваемого инструментария. Формулируются имеющиеся противоречия, вытекающие из них задачи исследования и ожидаемые результаты с соответствующей им новизной, практической ценностью и теоретической значимостью. Обсуждаются перспективы организации риск-анализа исследуемых контентов и использование его результатов для выработки рекомендаций по разграничению корпоративного доступа к информации.

Ключевые слова: контент, соцсеть, риск, парсинг, персонал, корпорация, доступ.

GOAL-SETTING OF PROJECT ACTIVITIES TO CREATE TOOLS FOR AUTOMATED IDENTIFICATION AND RISK ANALYSIS OF DESTRUCTIVE CONTENT AFFILIATED WITH CORPORATE PERSONNEL

A.G. Ostapenko, I.A. Bokov, S.V. Likhobabin, D.S. Yasenko, E.Y. Chapurin

Video, audio and graphic content of social networks are considered as a factor in ensuring information security of corporations. The goal-setting of project activities is carried out to create automated tools for identifying and risk analysis of the above-mentioned content, including parsing of social network resources, selection of collected content based on signs of destructiveness and their risk analysis to develop recommendations for delimiting access to corporate information. The relevance of the project activity is evaluated, analogues are investigated, architecture and algorithms of the created tools are proposed. The existing contradictions are formulated, the research tasks arising from them and the expected results with their corresponding novelty, practical value and theoretical significance. The prospects of organizing a risk analysis of the studied content and the use of its results to develop recommendations on the differentiation of corporate access to information are discussed.

Keywords: content, social network, risk, parsing, personnel, corporation, access.

DOI 10.36622/VSTU.2023.4.26.002
УДК 004.056

ЦЕЛЕПОЛАГАНИЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПО СОЗДАНИЮ ИНСТРУМЕНТАРИЯ АВТОМАТИЗАЦИИ ВЫЯВЛЕНИЯ И РЕГУЛИРОВАНИЯ РИСКОВ ДЕВИАНТНОГО ПОВЕДЕНИЯ СОТРУДНИКОВ КОРПОРАЦИЙ

А.Г. Остапенко, А.Г. Зимницкий, Е.А. Москалева

На основе всестороннего исследования предметной области обоснована актуальность создания инструментария выявления и регулирования рисков девиантного поведения сотрудников корпорации в контексте обеспечения их безопасности. Рассмотрение аналогов позволило осуществить целеполагание проектной деятельности по линейке взаимно однозначного соответствия выявленных противоречий, поставленных задач, ожидаемых результатов, их новизны, практической ценности и теоретической значимости. В соответствии с вышеизложенным предлагается архитектура создаваемого инструментария, включающая разнообразные библиотеки и модули, осуществляется демонстрация их использования на практических примерах автоматизированного анализа мимических эмоций (злость, отвращение, страх, радость, грусть, удивление и др.) человека.

Ключевые слова: риск, девиантное поведение, корпорация, целеполагание, эмоции.

GOAL-SETTING OF THE PROJECT ACTIVITY ON CREATION OF TOOLS FOR AUTOMATING THE DETECTION AND REGULATION RISKS OF DEVIANT BEHAVIOR OF CORPORATE EMPLOYEES

A.G. Ostapenko, A.G. Zimnitsky, E.A. Moskaleva

Based on a comprehensive study of the subject area, the relevance of creating tools for identifying and regulating the risks of deviant behavior of corporate employees in the context of ensuring their safety is substantiated. Consideration of analogues allowed to realize the goal-setting of project activities according to the line of mutually one-valued correspondence of the revealed contradictions, set tasks, expected results, their novelty, practical value and theoretical significance. In accordance with the above, the architecture of the created toolkit including various libraries and modules is proposed, their use is demonstrated on practical examples of automated analysis of human facial emotions (anger, disgust, fear, joy, sadness, surprise, etc).

Key words: risk, deviant behavior, corporation, goal setting, emotions.

DOI 10.36622/VSTU.2023.4.26.003
УДК 004.056

ДЕСТРУКТИВНЫЕ ИДЕОЛОГИИ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ СОЦИАЛЬНЫХ СФЕР

А.С. Овчинский, К.К. Борзунов

В условиях цифровой трансформации социальных сфер угрозы информационной безопасности связываются с негативными воздействиями на сознание людей и, в первую очередь, с деструктивными идеологиями. Значение идеологии в жизни общества сопоставляется с ролью информации. Представление идеологии в универсальной системе информационных координат высвечивает ее как правовую функцию, а именно ее роль в обосновании поведенческих реакций людей в самых разнообразных ситуациях. Анализируются истоки возникновения деструктивных идеологий. Комплексный подход позволяет связать и системно представить в универсальных координатах основные направления национально-этнического, религиозного и политического экстремизма. Обсуждаются деструктивные последствия противоборства основных мировых идеологий. Отмечается необходимость формирования и накопления идеологических ресурсов в противодействии социальной деструкции и обеспечении государственного суверенитета в ментально-когнитивной информационной войне уже с учетом угроз создаваемых систем генеративного искусственного интеллекта.

Ключевые слова: информационная безопасность, деструктивные идеологии, система координат, экстремизм, терроризм, религиозные доктрины, либерализм, консерватизм, социализм, искусственный интеллект, информационная война.

DESTRUCTIVE IDEOLOGIES AS A THREAT INFORMATION SECURITY IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF SOCIAL SPHERES

A.S. Ovchinsky, K.K. Borzunov

In the conditions of digital transformation of social spheres threats to information security are associated with negative impacts on people's consciousness and, first of all, with destructive ideologies. The importance of ideology in the life of society is compared with the role of information. The representation of ideology in a universal system of information coordinates highlights it as a matrix of justification of the right to a particular activity, to actions and deeds, to a way of life and thoughts. The origins of destructive ideologies are analyzed. An integrated approach allows us to link and systematically present in universal coordinates the main directions of national-ethnic, religious and political extremism. The destructive consequences of the confrontation of the main world ideologies are discussed. The necessity of formation and accumulation of ideological resources in countering social destruction and ensuring state sovereignty in the mental and cognitive information warfare is noted.

Keywords: information security, destructive ideologies, coordinate system, extremism, terrorism, religious doctrines, liberalism, conservatism, socialism, artificial intelligence, information warfare.

DOI 10.36622/VSTU.2023.4.26.004
УДК 004.056.47

ИНФОРМАЦИОННАЯ КАРТА КИБЕРКОНФЛИКТА «ПАЛЕСТИНА-ИЗРАИЛЬ»

А.Л. Сердечный, А.Г. Остапенко

Процессы информационного противоборства в киберпространстве тесно связаны с глобальной политической обстановкой. Риски компьютерных атак на государственные, промышленные, финансовые и частные информационные системы возрастают с обострением конфликтов между государствами в том числе в результате активизации политически мотивированных хакеров (хактивистов). За последние годы данный источник угроз превратился в хорошо организованную силу, способную проводить сложные и долговременные операции, действуя совместно с киберпреступниками и APT-группировками. В настоящей статье представлены результаты исследования киберконфликта «Палестина-Израиль», которое направлено на выявление скрытых связей между субъектами рассматриваемого конфликта. Исследование проводилось с помощью метода информационного картографирования, позволившего структурировать сведения от более чем 150 группировок хактивистов из стран Арабского и Индо-Тихоокеанского регионов. В результате информационно-картографического анализа были получены оценки обстановки, сложившейся в киберпространстве рассматриваемых регионов, а также сформирован набор данных о деятельности соответствующих хактивистких группировок за период с 6 октября по 11 ноября 2023 года.

Ключевые слова: хактивисты, информационная карта, кибервойна, Палестина-Израиль.

INFORMATION MAP OF THE CYBER CONFLICT “PALESTINE-ISRAEL”

A.L. Serdechnyi, A.G. Ostapenko

The processes of information warfare in cyberspace are closely related to the global political situation. The risks of computer attacks on government, industrial, financial and private information systems are increasing with the escalation of conflicts between states, including as a result of the intensification of politically motivated hackers (hacktivists). In recent years, this threat source has become a well-organized force capable of conducting complex and long-term operations, working in conjunction with cybercriminals and APT groups. This article presents the results of a study of the Palestine-Israel cyber conflict, which is aimed at identifying hidden connections between the subjects of the conflict under consideration. The study was conducted using the information mapping method, which made it possible to structure information from more than 150 hacktivist groups from the countries of the Arab and Indo-Pacific regions. As a result of the information and cartographic analysis, assessments of the situation in cyberspace in the regions under consideration were obtained, and a set of data on the activities of the corresponding hacktivist groups for the period from October 6 to November 11, 2023 was generated.

Keywords: hacktivists, information map, cyberwar, Palestine-Israel.

DOI 10.36622/VSTU.2023.4.26.005
УДК 519.766.4

КИТАЙСКИЙ ВЗГЛЯД НА РАЗВИТИЕ И БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА

В.А. Минаев, Е.С. Поликарпов

Цель исследования состоит в раскрытии взгляда экспертов из Китайской Народной Республики (КНР) на современные направления развития и обеспечения безопасности киберпространства. Обсуждаются важные аспекты концепции развития Интернет-державы, базируясь на стимулировании Китаем цифровой экономики, формировании чистой и надежной онлайн-среды, обеспечении безопасности киберпространства. Приводятся результаты анализа современного развития в стране, делается вывод о необходимости сотрудничества с КНР и масштабирования ее достижений при создании открытого, безопасного и устойчивого киберпространства. Указываются базовые направления формирования единого киберсообщества: активное содействие цифровой индустриализации и цифровой трансформации общества; развитие сообщества безопасности киберпространства; построение коллективной кибер ответственности; достижение общих кибер интересов. Среди основных принципов создания единого киберпространства рассматриваются четыре: соблюдение цифрового суверенитета, сохранение стабильности и безопасности киберпространства, содействие открытости и сотрудничеству, поддержание киберпорядка. Обсуждается проблема чистоты цифрового контента в Интернет, говорится о том, что безопасность в киберпространстве – многомерный объект, которому присущи: позитивная энергия в Интернете, разнообразие цифровой культуры, передовые средства онлайн-коммуникации и обработки данных, киберэкосистемные представления Сети, продвижение Интернет-цивилизации, развитие работы онлайн-платформ.

Ключевые слова: Китай, Интернет, цифровое развитие, безопасность, киберпространство.

THE CHINESE VIEW ON THE DEVELOPMENT AND SECURITY OF CYBERSPACE

V.A. Minaev, E.S. Polikarpov

The purpose of the article is to reveal the view of experts from the People's Republic of China (PRC) on modern trends in the development and security of cyberspace. The important aspects of the concept of China's development of an Internet power are discussed, based on stimulating the digital economy, forming a clean and reliable online environment, and ensuring the security of cyberspace. The results of the modern development analysis in the country are presented, the conclusion is made about the need for cooperation with China and scaling up its achievements in creating an open, secure and sustainable cyberspace. The basic directions of the unified cyber community formation are indicated: active promotion of digital industrialization and digital transformation of society; development of the cyberspace security community; building collective cyber responsibility; promotion of common cyber interests. Among the basic principles of creating a unified cyberspace, four are considered: respect for digital sovereignty, preservation of stability and security of cyberspace, promotion of openness and cooperation, and maintenance of cyber order. The problem of digital content purity on the Internet is discussed, it is said that security in cyberspace is a multidimensional object that is inherent in: positive energy on the Internet, the diversity of digital culture, advanced means of online communication and data processing, cyber-ecosystem representations of the Network, the promotion of Internet civilization, the development of online platforms.

Keywords**:** China, Internet, digital development, security, cyberspace.

DOI 10.36622/VSTU.2023.4.26.006
УДК 004.735

МОДЕЛЬ ПЕРЕХВАТА И ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, П.А. Анцупов, А.Г. Чурсин

Беспроводные сети широко используются во всех сферах нашей жизни обеспечивая доступ к интернету и другим сетевым ресурсам. На базе беспроводных сетей строятся сети интернета вещей, а в связи с экспоненциальным распространением включения в Интернет различных вещей, устройств и датчиков возникают различные риски безопасности систем, в том числе связанные с перехватом информации в беспроводных сетях. Цель работы – защита информации беспроводных IoT устройств от атак, направленных на выведение из строя и до ведения до отказа вещей в сети предприятия. В статье предложена модель перехвата информации, состоящая из беспроводной распределенной компьютерной сети предприятия, имеющей IoT устройства, в которые после успешной атаки загружается вредоносная программа Mirai. В процессе исследования предложена модель защиты информации с применением системы обнаружения вторжения.

Ключевые слова: беспроводные сети, Интернет Вещей, перехват и защита информации, Wi-Fi 6, распределенные сети, DDoS, системы обнаружения вторжений, IDS.

A MODEL OF INTERCEPTION AND PROTECTION OF INFORMATION IN DISTRIBUTED COMPUTER NETWORKS OF THE INDUSTRIAL INTERNET OF THINGS

S.A. Ermakov, P.A. Antsupov, A. G. Chursin

Wireless networks are widely used in all spheres of our life providing access to the Internet and other network resources. The Internet of Things networks are being built on the basis of wireless networks, and due to the exponential spread of the inclusion of various things, devices and sensors on the Internet, various security risks of systems arise, including those associated with the interception of information in wireless networks. The purpose of the work is to protect the information of wireless IoT devices from attacks aimed at disabling and failing things in the enterprise network. The article proposes a model of information interception consisting of a wireless distributed computer network of an enterprise having IoT devices into which, after a successful attack, the Mirai malware is loaded. In the course of the research, a model of information protection using an intrusion detection system is proposed.

Keywords: wireless networks, Internet of Things, interception and protection of information, Wi-Fi 6, distributed networks, DDoS, intrusion detection systems, IDS.

DOI 10.36622/VSTU.2023.4.26.007
УДК 004.056.5

РАЗРАБОТКА РЕСУРСНО-ЭФФЕКТИВНОЙ ТЕХНОЛОГИИ ДИНАМИЧЕСКОГО МАСКИРОВАНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РЕЛЯЦИОННЫХ БАЗАХ ДАННЫХ

В.П. Лось, Д.Д. Маланьин

Защита конфиденциальной и персональной информации является актуальной задачей информационной безопасности. В особенности это касается реляционных баз данных, которые широко используются в различных сферах деятельности: от банковского сектора до интернет-магазинов. Нарушение конфиденциальности часто становится проблемой безопасности данных, особенно при работе с персональными данными клиентов. В статье рассмотрена методика построения ресурсно-эффективной, с точки зрения используемой постоянной памяти сервера базы данных, технологии динамического маскирования конфиденциальной информации в реляционных структурах баз данных. Методика позволяет обезопасить данные при обращении к ним аналитических сервисов и приложений, сохраняя при этом функциональные возможности.

Ключевые слова: информационная безопасность, системы управления базами данных, маскирование данных.

DEVELOPMENT OF RESOURCE-EFFICIENT TECHNOLOGY DYNAMIC MASKING OF CONFIDENTIAL INFORMATION IN RELATIONAL DATABASES

V.P. Los, D.D. Malanin

The task of protecting conference and personal information is an urgent task of information security. This is especially true for relational databases, which are widely used in various spheres of activity: from the banking sector to online stores. Violation of confidentiality often becomes a problem of data security, especially when working with personal data of clients. In the article we consider the method of building resource-efficient (in terms of used permanent memory of the database server) technology of dynamic masking of confidential information in relational structures of databases. The technique allows to secure the data when analytical services and applications access them, while preserving functional capabilities.

Keywords: information security, database management systems, data masking.

DOI 10.36622/VSTU.2023.4.26.008
УДК 004.056

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ, ОСНОВАННЫХ НА ПРИМЕНЕНИИ БЕСПРОВОДНЫХ СЕТЕЙ

Ю.Ю. Громов, П.И. Карасев, А.И. Елисеев, Н.С. Кибец

В работе рассмотрены основные методы защиты от атак на информационные системы, использующие беспроводные сети Wi-Fi. При описании каждого из них были разобраны причины возникновения уязвимостей, которые и повлекли за собой возможность компрометации сети информационной системы со стороны злоумышленника, а также приведены возможные способы их исправления. Были рассмотрены уязвимости таких типов сетей, как WPA2 Personal и WPA2 Enterprise, но больший акцент был сделан именно на первом типе, так как такие сети более повсеместны, их можно встретить повсюду. В первую очередь информация о данных недостатках безопасности представлена для ознакомления, ведь для того, чтобы понять, как обезопасить свою беспроводную сеть, для начала следует выяснить, какие уязвимости существуют и как от них можно защититься. Кроме того, в статье была рассмотрена роль беспроводной сети в общей модели безопасности локальной сети.

Ключевые слова: Wi-Fi, перехват трафика, ИБ, SSID, WPA-2, WEP, handshake, PNL, WPA/WPA2-Personal (PSK), WPA/WPA2-Enterprise (MGT), Man-in-the-Middle, WPS, Brute force, WPS Pixie Dust, PSK, MAC адрес.

METHODS FOR PROTECTING INFORMATION SYSTEMS BASED ON WIRELESS NETWORKS

Yu.Yu. Gromov, P.I. Karasev, A.I. Eliseev, N.S. Kibets

The paper discusses the main methods of protection against attacks on information systems using wireless Wi-Fi networks. When describing each of them, the reasons for the occurrence of vulnerabilities, which entailed the possibility of compromising the information system network by an attacker, were analyzed, and possible ways to correct them were also given. The vulnerabilities of such types of networks as WPA2 Personal and WPA2 Enterprise were considered, but greater emphasis was placed on the first type, since such networks are more ubiquitous and can be found everywhere. First of all, information about these security flaws is presented for your information, because in order to understand how to secure your wireless network, you first need to find out what vulnerabilities exist and how you can protect yourself from them. In addition, the article examined the role of a wireless network in the general local network security model.

Keywords: Wi-Fi, Traffic interception, IBM, SSID, WPA-2, WEP, Handshake, PNL, WPA/WPA2-Personal (PSK), WPA/WPA2-Corporate (MGT), Man-in-the-Middle, WPS, Brute force, WPS Pixie Dust, PSK, MAC Address.

DOI 10.36622/VSTU.2023.4.26.009
УДК 004.056

АНАЛИЗ ЗАЩИЩЕННОСТИ КОМПОНЕНТОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ, ПОСТРОЕННОЙ НА БЕСПРОВОДНЫХ СЕТЯХ

Ю.Ю. Громов, П.И. Карасев, А.И. Елисеев, Е.О. Карамышева, Н.С. Кибец

В работе рассмотрена безопасность информационных систем, построенных на беспроводных технологиях, представлены нормативные документы, которые содержат в себе требования и рекомендации к настройке информационных систем для предотвращения их дальнейшей компрометации со стороны внешних нарушителей. Помимо этого, была рассмотрена история Wi-Fi, а именно то, как эволюционировали беспроводные сети по скорости, по безопасности с точки зрения шифрования передаваемых в беспроводной среде данных. Кроме того, был проведен экскурс в устаревшие алгоритмы шифрования. Одной из ключевых задач стало создание стенда, с помощью которого удалось убедиться в уязвимости старых протоколов к современным угрозам. В статье также представлен аудит безопасности экспериментальной тестовой сети, а также описан процесс его проведения с указанием использующихся утилит. По результатам тестирования представлены рекомендации по обеспечению безопасности таких информационных систем.

Ключевые слова: информационные системы беспроводные сети, Wi-Fi, уязвимость, безопасность, перехват трафика, ИБ, SSID, WPA-2, WEP, handshake, PNL, WPA/WPA2-Personal (PSK), WPS Pixie Dust.

ANALYSIS OF THE SECURITY OF COMPONENTS OF AN INFORMATION SYSTEM BUILT ON WIRELESS NETWORKS

Y.Y. Gromov, P.I. Karasev, A.I. Eliseev, E.O. Karamysheva, N.S. Kibets

The paper examines the security of information systems built on wireless technologies, presents regulatory documents that contain requirements and recommendations for setting up information systems to prevent their further compromise by external violators. In addition, the history of Wi-Fi was reviewed, namely how wireless networks have evolved in terms of speed, security, and in terms of encryption of data transmitted in a wireless environment. In addition, an excursion into outdated encryption algorithms was conducted. One of the key tasks was the creation of a stand, with the help of which it was possible to verify the vulnerability of old protocols to modern threats. The article also presents a security audit of an experimental test network, and also describes the process of conducting it, indicating the utilities used. Based on the testing results, recommendations for ensuring the security of such information systems are presented.

KEYWORDS: wireless networks, Wi-Fi, accessibility, security, intercept traffic, IB, SSID, WPA2, WEP, handshake, ONLY, WPA/WPA2-Personal (PSK), WPS Pixie Dust.

DOI 10.36622/VSTU.2023.4.26.010
УДК 004.056.5

НЕЙРОСЕТЕВЫЕ ЗАДАЧИ И КОМПЕТЕНЦИИ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПО СОЗДАНИЮ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Г.А. Остапенко, А.П. Васильченко

Рассматриваются противоречия инструментальной базы проектирования атакуемых автоматизируемых информационных систем (АИС). Обосновывается объективная необходимость использования в проектной деятельности искусственных нейросетей в качестве интеллектуальной поддержки организационно- правовых и научно-технических управленческих решений по защите информации в АИС. Осуществляется целеполагание исследования в условиях неуклонно растущего многообразия компьютерных атак и революционного развития искусственного интеллекта. Формулируются задачи и ожидаемые результаты, а также - необходимые для их достижения нейросетевые компетенции, формирование и развитие которых представляется актуальным условием успеха исследований и разработок в области интеллектуализации создаваемых и эксплуатируемых АИС.

Ключевые слова: нейросети, автоматизированные информационные системы, компьютерные атаки, компетенции.

NEURAL NETWORK TASKS AND COMPETENCIES OF PROJECT ACTIVITY FOR CREATION OF SECURE AUTOMATED INFORMATION SYSTEMS

G.A. Ostapenko, A.P. Vasilchenko

The contradictions of the instrumental base of designing the attacked automated information systems (AIS) are considered. The objective necessity of using artificial neural networks in project activities as intellectual support for organizational, legal, scientific and technical management decisions on information security in AIS is substantiated. The goal-setting of the research is carried out in the conditions of a steadily growing variety of computer attacks and the revolutionary development of artificial intelligence. The tasks and expected results are formulated, as well as the neural network competencies necessary for their achievement, the formation and development of which seems to be an urgent condition for the success of research and development in the field of intellectualization of created and operated AIS.

Keywords: neural networks, automated information systems, computer attacks, competencies.

DOI 10.36622/VSTU.2023.4.26.011
УДК 004.056.47

МЕТОД ИНФОРМАЦИОННО-КАРТОГРАФИЧЕСКОГО АНАЛИЗА АКТИВНОСТИ ГРУППИРОВОК ХАКТИВИСТОВ

А.Л. Сердечный, А.Г. Остапенко

Объективное понимание ландшафта угроз является необходимым условием для выработки эффективных мер предотвращения компьютерных инцидентов или снижения негативных последствий в случае их наступления. В статье предлагается метод, который обеспечивает такое понимание для угроз, связанных с действиями политически мотивированных группировок (хактивистов). Метод основан на использовании информационных карт для визуализации сложных взаимосвязей между такими группами. В рамках описания метода определён процесс построения и анализа информационных карт, включающий сбор сведений о действиях хактивистов в публичном пространстве, формирование графа связей и размеченного ландшафта информационной карты, с помощью которых проводится анализ явных и скрытых зависимостей между группировками, их сообществами, а также атакуемыми объектами. С помощью информационных карт удобно осуществлять мониторинг за большим количеством источников и событий в рамках глобальных киберконфликтов, затрагивающих несколько сотен групп из различных стран и регионов. В результате информационно-картографического анализа активности группировок хактивистов могут быть заранее определены направления их атак, что позволяет своевременно повысить бдительность групп реагирования на инциденты и обеспечить координированное взаимодействие в информационном пространстве.

Ключевые слова: информационно-картографический анализ, хактивисты, информационная карта.

THE INFOCARTOGRAPHIC ANALYSIS METHOD OF HACKTIVIST ACTION

A.L. Serdechnyi, A.G. Ostapenko

An objective understanding of the threat landscape is a prerequisite for developing effective measures to prevent computer incidents or reduce negative consequences in the event of their occurrence. The article proposes a method that provides such an understanding for threats related to the actions of politically motivated groups (hacktivists). The method is based on the use of information maps to visualize complex relationships between such groups. As part of the description of the method, the process of constructing and analyzing information maps is defined, including collecting information about the actions of hacktivists in public space, forming a graph of connections and a marked landscape of the information map, with the help of which the analysis of explicit and hidden dependencies between groups, their communities, as well as the attacked objects is carried out. With the help of information maps, it is convenient to monitor a large number of sources and events within the framework of global cyber conflicts affecting several hundred groups from different countries and regions. As a result of the infocartographic analysis of the activity of hacktivist groups, the directions of their attacks can be determined in advance, which makes it possible to increase the vigilance of incident response teams in a timely manner and ensure coordinated interaction in the information space.

Keywords: infocartographic analysis, hacktivists, information map.

DOI 10.36622/VSTU.2023.4.26.012
УДК 004.056.5

МЕТОДИКИ РЕГЛАМЕНТАЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АТАКУЕМЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Г.А. Остапенко, А.П. Васильченко

Рассматривается защита корпоративных информационных ресурсов и сетей от многообразия кибератак. Акцентируется внимание на методиках построения риск-ландшафта и частных регламентов (реагирования на несанкционированные вторжения, ликвидации их негативных последствий) обеспечения информационной безопасности защищаемых автоматизированных систем. В этом контексте предлагаются научно-методические решения для построения риск-ландшафта рассматриваемых разновидностей атак и вышеупомянутой регламентации в отношении сочетаний вектор атаки-уязвимость. Излагаются принципиальные моменты функционального и структурного согласования элементов создаваемых регламентов в плане их сквозной горизонтали, обеспечивающей взаимно однозначное соответствие злоумышленных действий и мер ликвидации их негативных последствий. Инструментарий противодействия целому классу кибератак определяется как совокупность сформированных частных регламентов.

Ключевые слова: защита, ресурсы, сети, системы, регламент, риск, атака, уязвимость.

METHODS FOR REGULATING INFORMATION SECURITY OF ATTACKED AUTOMATED SYSTEMS

G.A. Ostapenko, A.P. Vasilchenko

The protection of corporate information resources and networks from a variety of cyber attacks is considered. Attention is focused on methods for constructing a risk landscape and private regulations (responding to unauthorized intrusions, eliminating their negative consequences) to ensure the information security of protected automated systems. In this context, scientific and methodological solutions are proposed for constructing a risk landscape for the types of attacks under consideration and the above-mentioned regulation regarding attack vector-vulnerability combinations. The fundamental points of functional and structural coordination of the elements of the created regulations are outlined in terms of their end-to-end horizontal, ensuring a one-to-one correspondence between malicious actions and measures to eliminate their negative consequences. The tools for countering a whole class of cyber attacks are defined as a set of developed private regulations.

Keywords: protection, resources, networks, systems, regulations, risk, attack, vulnerability.