DOI 10.36622/VSTU.2021.24.3.001
УДК 004.492.2

КИБЕРПРОСТРАНСТВО КАК ОБЪЕКТ ИССЛЕДОВАНИЯ И ЗАЩИТЫ. ЧАСТЬ 1

А.Л. Сердечный

Работа посвящена описанию киберпространства как защищаемого объекта, обладающего уникальными свойствами по сравнению с другими видами пространств (водным, земным, воздушным и космическим). В рамках проведённых исследований рассмотрены различные определения данного понятия и выделены его основные аспекты. Рассмотрение киберпространства в этих аспектах позволило выявить основные закономерности его генезиса и эволюции о которых также рассказывается в настоящей статье. Также было показано, что сложность и размер киберпространств требует особых подходов его изображения и исследования, в том числе, через анализ субъектов, которые его порождают, а также действуют в нём. Фактически предлагается новый взгляд на специфическое пространство, порожденное человечеством, которое сегодня проникло во все сферы общественной деятельности и остро нуждается в защите и глубоком исследовании (в том числе и картографическими методами).

Ключевые слова: киберпространство, генезис киберпространства, эволюция киберпростарнства, представление киберпростарнства.

CYBERSPACE AS AN OBJECT OF RESEARCH AND PROTECTION. PART 1

A.L. Serdechnyy

The paper focuses on describing cyberspace as a protected object that has unique properties compared to other types of space (aquatic, terrestrial, air and space). Within the framework of the conducted research different definitions of this concept have been considered and its main aspects have been highlighted. Consideration of cyberspace in these aspects allowed us to identify the main patterns of its genesis and evolution, which are also described in this article. It was also shown that the complexity and size of cyberspaces requires special approaches to its portrayal and study, including through the analysis of the actors that generate it as well as act in it. In fact, it offers a new perspective on the specific space generated by mankind, which has now penetrated all spheres of social activity and is in dire need of protection and in-depth study (including by mapping methods).

Keywords: cyberspace, genesis of cyberspace, evolution of cyberspace, representation of cyberspace.

DOI 10.36622/VSTU.2021.24.3.002
УДК 004.492.2

КИБЕРПРОСТРАНСТВО КАК ОБЪЕКТ ИССЛЕДОВАНИЯ И ЗАЩИТЫ. ЧАСТЬ 2

А.Л. Сердечный

В статье рассматриваются основные аспекты исследования киберпространства: территория, сетевое представление и расстояние между расположенными в нём объектами. Показана возможность многокомпонентного представления киберпространства в виде системы уровней взаимосвязанных объектов: физического, информационного и социального. Обсуждаются возможности регулирования защищаемого киберпространства со стороны его различных субъектов. Уделяется внимание большим данным, циркулирующим в киберпространстве. Рассматриваются возможные подходы к исследованию защищаемого киберпространства, включая шаблонно-онтологический, теоретико-игровой, сетевой и геопространственный подходы. Приводятся преимущества и ограничения каждого из них. Особое внимание уделяется картографической методологии исследования защищаемого киберпространства, в связи с чем в качестве иллюстрации его основных идей рассматривается информационная карта поиска научных публикаций по теме «Картография защищаемого киберпространства». В заключении формируются задачи разработки реализации картографической методологии исследования защищаемого киберпространства.

Ключевые слова: защищаемое киберпространство, территория киберпространства, большие данные, информационная карта.

CYBERSPACE AS AN OBJECT OF RESEARCH AND PROTECTION. PART 2

A.L. Serdechnyy

The article discusses the main aspects of cyberspace research: area, the network representation and the distance between the objects located in it. The possibility of multi-component representation of cyberspace as a system of levels of interconnected objects is shown: physical, informational and social. Possibilities of regulating protected cyberspace by its various actors are discussed. Attention is paid to the big data circulating in cyberspace. Possible approaches to the study of defensible cyberspace, including template-ontological, game-theoretic, network and geospatial approaches, are examined. The advantages and limitations of each are given. Particular attention is paid to the cartographic methodology of protected cyberspace research, and in this regard, an information map of research publications search on “Mapping of Protected Cyberspace” is considered as an illustration of its main ideas. The conclusion formulates the objectives of developing the implementation of a mapping methodology for the study of protected cyberspace.

Keywords: protected cyberspace, cyberspace territory, big data, information map.

DOI 10.36622/VSTU.2021.24.3.003
УДК 004.056

ИМИТАЦИЯ ФУНКЦИОНИРОВАНИЯ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РЕАЛИЗАЦИИ КИБЕРАТАК

В.А. Минаев, Е.С. Поликарпов

Статья посвящена проблеме моделирования работы центра информационной безопасности предприятия (ЦИПБ) в условиях реализации кибератак. Имитационная модель позволяет решать широкий спектр задач, в частности, задач управления временем обработки сообщений об инцидентах безопасности, оптимизации ресурсного обеспечения информационной безопасности предприятия, ее прогнозирования. Показано, что для решения указанных хорошо применимы методы дискретно-событийного моделирования. Дискретно-событийная модель ЦИБП отражает современные тренды в области технологического обеспечения информационной безопасности предприятий и организаций; учитывает наиболее существенные факторы, влияющих на характеристики информационной безопасности предприятий; обеспечивает баланс между требуемой точностью результатов моделирования и сложностью модели; отличается универсальностью, адаптивностью для решения многих задач управления информационной безопасностью, гибкостью разработки моделей в современной среде имитационного моделирования. В качестве среды имитационного моделирования выбрано программное обеспечение отечественного производства Anylogic, позволившее проигрывать различные сценарии кибератак на ЦИБП, помогающее качественно интерпретировать результатов реализации моделей, провести различные виды имитационных экспериментов, в том числе – по вариации параметров моделей, анализу их чувствительности, оптимизации ресурсного обеспечения информационной защиты. Сделан вывод, что дальнейшим развитием исследования ЦИБП предприятий является уточнение и детализация модели, структуры ее блоков и содержания сообщений о компьютерных инцидентах.

Ключевые слова: кибератака, предприятие, информационная безопасность, дискретно-событийное моделирование, SIEM-система, SOC-центр, имитация.

SIMULATION OF INFORMATION SECURITY CENTER FUNCTIONING IN THE CONTEXT OF CYBER ATTACKS REALIZATION

V.A. Minaev, E.S. Polikarpov

The article is devoted to the problem of modeling the functioning of the Enterprise Information Security Center (EISC) in the context of the realization of cyber attacks. The simulation model allows you to solve a wide range of tasks, in particular, the tasks of managing the processing time of security incident reports, optimizing the resource support of enterprise information security, and forecasting it. It is shown that the methods of discrete-event modeling are applicable for solving these problems. The discrete-event model of EISC reflects modern trends in the field of technological support of information security of enterprises and organizations; takes into account the most significant factors that affect the characteristics of information security of enterprises; provides a balance between the required accuracy of modeling results and the complexity of the model; is characterized by versatility, adaptability to solve many problems of information security management, flexibility of model development in the modern environment of simulation modeling. As a simulation environment, Anylogic software of domestic production was chosen, which made it possible to play various scenarios of cyber attacks on the EISC, which helps to qualitatively interpret the results of the implementation of models, to conduct various types of simulation experiments, including the variation of model parameters, the analysis of their sensitivity, and the optimization of the resource provision of information protection. It is concluded that the further development of the study of the EISC of enterprises is the refinement and detailing of the model, the structure of its blocks and the content of messages about computer incidents.

Keywords: cyber attack, enterprise, information security, discrete-event modeling, SIEM-system, SOC-center, simulation.

DOI 10.36622/VSTU.2021.24.3.004
УДК 004.056

ПРИМЕНЕНИЕ ГЛУБИННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ВЫЯВЛЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНЫХ МЕДИА

В.А. Минаев, Е.С. Поликарпов, А.В. Симонов

Цель исследования состоит в разработке методики и поиске эффективного алгоритма выявления деструктивного контента в кратких публикациях и комментариях в социальных медиа. Проведен обзор существующих решений для выявления деструктивного контента, описаны их преимущества и недостатки в контексте решаемой задачи. Сформированы составные экспериментальные корпуса текстов по темам: реабилитация нацизма, антисемитизм, радикальный ислам. Проведена нормализация корпусов, используя методы стемминга и лемматизации. Осуществлена операция векторизации нормализованных корпусов методами мешка слов (BoW), TF-IDF и слоем искусственных нейронных сетей (ИНС). Построены архитектуры глубинных ИНС: сверточной нейронной сети (CNN), рекуррентной нейронной сети с долгой краткосрочной памятью (LSTM), рекуррентной нейронной сети с механизмом вентилей (GRU). Проведены эксперименты по классификации сформированных корпусов текстов с использованием созданных ИНС и традиционных методов машинного обучения. Произведена интерпретация полученных результатов экспериментов и обосновано применение глубинных ИНС при решении поставленной задачи. Сделан вывод о целесообразности использования полученных результатов структурами, занятыми выявлением и удалением деструктивного контента.

Ключевые слова: информационная безопасность, социальные медиа, деструктивный контент, нейронные сети, глубокое обучение, классификация текста.

APPLICATION OF DEEP NEURAL NETWORKS TO IDENTIFY DESTRUCTIVE CONTENT IN SOCIAL MEDIA

V.A. Minaev, E.S. Polikarpov, A.V. Simonov

The purpose of the research is to develop a methodology and search for an effective algorithm for identifying destructive content in short publications and comments in social media. The review of existing solutions for identifying destructive content is carried out, their advantages and disadvantages are described in the context of the problem being solved. Composite experimental corpuses of texts on the following topics were formed: rehabilitation of Nazism, anti-Semitism, and radical Islam. The normalization of the cases was carried out using the methods of stemming and lemmatization. The operation of vectorization of normalized corpora by the methods of a bag of words (BoW), TF-IDF and a layer of artificial neural networks (INS) is carried out. The architectures of deep INS are constructed: convolutional neural network (CNN), recurrent neural network with long short-term memory (LSTM), recurrent neural network with a gate mechanism (GRU). Experiments were conducted on the classification of the generated text corpora using the created INS and traditional machine learning methods. The interpretation of the obtained experimental results is made and the use of deep INS in solving the problem is justified. The conclusion is made about the expediency of using the obtained results by structures engaged in identifying and removing destructive content.

Keywords: information security, social media, destructive content, neural networks, deep learning, text classification.

DOI 10.36622/VSTU.2021.24.3.005
УДК 004.492.2

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ КАРТОГРАФИИ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА. ЧАСТЬ 1

А.Л. Сердечный

Для определения понятия «информационная карта» осуществлен обзор основных этапов развития картографии в качестве инструментария, используемого для ориентации в окружающем пространстве, познания и планирования различных процессов, связанных с пространственными данными. С учетом данного обзора информационная карта определяется как цифровой объект, представляющий в пространстве исследуемое множество объектов, субъектов и процессов многомерного киберпространства на основе принципов: измеримости сходства объектов; близости изображений объектов, изображения контекста, воспроизводимости операций построения карты. Приводятся разноплановые примеры использования информационной карты в биологии, медицине, химии, социологии, интеллектуальном сотрудничестве и исторической науке. Тем самым обосновывается целесообразность информационного картографирования защищаемого киберпространства.

Ключевые слова: информационная карта, киберпространство, картография киберпространства.

CONCEPTUAL FRAMEWORK FOR PROTECTED CYBERSPACE MAPPING. PART 1

A.L. Serdechnyy

To define the concept of "information map", an overview of the main stages in the development of cartography as a tool used for orientation in the surrounding space, cognition and planning of various processes associated with spatial data is carried out. Taking into account this review, an information map is defined as a digital object representing in space the studied set of objects, subjects and processes of multidimensional cyberspace based on the principles: measurability of the similarity of objects; proximity of object images, context images, reproducibility of map building operations. Various examples of the use of the information card in biology, medicine, chemistry, sociology, intellectual cooperation and historical science are given. Thus, the expediency of information mapping of the protected cyberspace is substantiated.

Keywords: information map, cyberspace, cyberspace mapping.

DOI 10.36622/VSTU.2021.24.3.006
УДК 004.492.2

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ КАРТОГРАФИИ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА. ЧАСТЬ 2

А.Л. Сердечный

В работе типизированы задачи, для решения которых могут эффективно использоваться информационные карты, включая: разведку (исследование новых территорий, выявление скрытых элементов, установление противоборствующих сторон); планирование операций (анализ ресурсов сторон конфликтов, прокладка маршрута, прогнозирование последствий); мониторинг обстановки (координация взаимодействия, выявление изменений обстановки, вскрытие ошибок и дезинформации); представление знаний (обучение, структурированное хранение знаний, поиск информации). Рассматривается вербальная модель процесса информационно-картографического исследования. Обсуждаются методические и инструментальные аспекты информационного картографирования. Формируются задачи для реализации картографического подхода, включая: обоснование правил построения и анализа информационных карт; обоснование состава и структуры системы картографирования; разработку масштабируемой информационной карты защищаемого киберпространства.

Ключевые слова: картографическая разведка, информационная карта, картография киберпространства.

CONCEPTUAL FRAMEWORK FOR PROTECTED CYBERSPACE MAPPING. PART 2

A.L. Serdechnyy

In the work, tasks are typified, for the solution of which information maps can be effectively used, including: reconnaissance (exploration of new territories, revealing hidden elements, establishing opposing sides); planning of operations (analysis of the resources of the parties to conflicts, laying a route, forecasting events); monitoring the situation (coordinating interaction, identifying changes in the situation, revealing errors and misinformation); knowledge representation (training, structured knowledge storage, information retrieval). A verbal model of the information-cartographic research process is considered. Methodological and instrumental aspects of information mapping are discussed. The tasks for the implementation of the cartographic approach are formed, including: substantiation of the rules for the construction and analysis of information maps; substantiation of the composition and structure of the mapping system; development of a scalable information map of the protected cyberspace.

Keywords: mapping intelligence, information map, cyberspace mapping.

DOI 10.36622/VSTU.2021.24.3.007
УДК 004.056.55/003.26

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА – ПОДХОДЫ, ТЕХНОЛОГИЯ (ЧАСТЬ 1)

П.Ю. Филяк, И.А. Захаренков, И.С. Перевезенцев

В статье рассматривается подход к обеспечению информационной безопасности с позиций нового технологического уклада, основанного на широком использовании целого спектра современных методов и инструментов, характерных для информационного общества не в фазе его формировании, а на этапе интенсивного развития. Всемирный экономический форум в Давосе в 2016 году в докладах участников и итоговых документах обозначил и провозгласил четвертый технологический уклад, или инновационную экономику, также широко известную под брендом Индустрия 4.0. В технологическом плане это означает широкое использование одного из основных научно-технических направлений данного уклада – искусственного интеллекта (ИИ, Artificial Intelligence (AI)). Комплексная цифровая трансформация экономики и социальной сферы предусмотрена национальным проектом «Цифровая экономика Российской Федерации», отдельным разделом которой является обеспечение информационной безопасности цифровой экономики, что также предусматривает применение новых подходов и инструментов для решения данных задач, среди которых предусмотрено использование искусственного интеллекта.

Ключевые слова: цифровая экономика, цифровая трансформация, информация, информационное общество, информационная безопасность, искусственный интеллект, интерфейс, политика безопасности, политики доступа, идентификация, аутентификация, распознавание речи, распознавание образов, авторизация.

ENSURING INFORMATION SECURITY OF AN INFORMATION SYSTEM USING ARTIFICIAL INTELLIGENCE-APPROACHES, TECHNOLOGY (PART I)

P.Yu. Filyak, I.A. Zakharenkov, I.S. Perevezentsev

The article considers the approach to ensuring information security from the standpoint of a new technological structure based on the wide use of a whole range of modern methods and tools that are characteristic of the information society not in the phase of its formation, but at the stage of intensive development. The World Economic Forum in Davos in 2016, in the reports of the participants and the final documents, identified and proclaimed the fourth technological order, or innovative economy, also widely known under the brand Industry 4.0. In technological terms, this means the widespread use of one of the main scientific and technical directions of this way of life-artificial intelligence (AI). A comprehensive digital transformation of the economy and social sphere is provided for by the national project "Digital Economy of the Russian Federation", a separate section of which is to ensure the information security of the digital economy, which also provides for the use of new approaches and tools to solve these problems, among which the use of artificial intelligence is provided.

Keywords: digital economy, digital transformation, information, information society, information security, artificial intelligence, interface, security policy, access policies, identification, authentication, speech recognition, image recognition, authorization.

DOI 10.36622/VSTU.2021.24.3.008
УДК 004.056.55/003.26

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА – ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ (ЧАСТЬ 2)

П.Ю. Филяк, И.А. Захаренков, И.С. Перевезенцев

Предложена практическая реализация подхода к обеспечению информационной безопасности информационной системы на основе использования политик информационной безопасности, базирующихся на применении различных вариантов всех известных политик доступа к информации, которые, в свою очередь, реализуются путем имплементации платформ самых современных интерфейсов с помощью искусственного интеллекта (ИИ/ AI). Данные интерфейсы предполагают бесконтактную идентификацию и аутентификацию пользователя, в зависимости от заданных условий политик доступа, системы, правил и средств разграничения доступа к информационной системе. В частности, предусматривается идентификация и аутентификация с использованием системы визуализации и распознавания зрительных образов, а также с помощью распознавания речи, с учетом тембральных и модуляционных характеристик голоса, что обеспечивает высокую точность идентификации и аутентификации и степень достоверности при выполнении процедура авторизации, поскольку программная и аппаратная составляющая функций ИИ позволяет осуществлять многофакторный мониторинг за действиями пользователей и сортировать события в режиме online.

Ключевые слова: информация, информационное общество, информационная безопасность, цифровая экономика, искусственный интеллект, интерфейс, политика безопасности, политики доступа, идентификация, аутентификация, распознавание речи, распознавание образов, авторизация.

ENSURING INFORMATION SECURITY OF AN INFORMATION SYSTEM USING ARTIFICIAL INTELLIGENCE - PRACTICAL IMPLEMENTATION (PART 2)

P.Yu. Filyak, I.A. Zakharenkov, I.S. Perevezentsev

The practical implementation of an approach to ensuring the information security of an information system is proposed based on the use of information security policies based on the application of various variants of all known information access policies, which, in turn, are implemented by implementing the most modern interface platforms using artificial intelligence (AI/ AI). These interfaces assume contactless identification and authentication of the user, depending on the specified conditions of access policies, system, rules and means of access control to the information system. In particular, it provides for identification and authentication using a visual image visualization and recognition system, as well as using speech recognition, taking into account the timbral and modulation characteristics of the voice, which ensures high accuracy of identification and authentication and a degree of reliability when performing the authorization procedure, since the software and hardware component of the AI functions allows for multi-factor monitoring of user actions and sorting events online.

Keywords: information, information society, information security, digital economy, artificial intelligence, interface, security policy, access policies, identification, authentication, speech recognition, image recognition, authorization.

DOI 10.36622/VSTU.2021.24.3.009
УДК 004.056

МЕТОДИКА ОПРЕДЕЛЕНИЯ ЦЕННОСТИ ЗАЩИЩАЕМЫХ АКТИВОВ ДЛЯ АУДИТА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

О.М. Голембиовская, К.Е. Шинаков, Е.В. Кондрашова, А.П. Жолнеров

В статье рассматривается методика, связанная с определением ценности активов для аудита обеспечения информационной безопасности коммерческой организации. Помимо этого, предложен подход для прогнозирования нанесения возможного ущерба рассматриваемым активам. Предлагаемую методику целесообразно применять службам безопасности предприятия с целью выявления недостатков системы защиты и выполнению различных мер по нейтрализации или минимизации вероятности реализации возможных угроз. Определение ценности активов организации является важным этапом аудита. Основными активами коммерческой организации с точки зрения обеспечения информационной безопасности являются: информационная система, сервер, компьютеры и иное оборудование для работы сотрудников, внутренние базы данных. Процедура определения ценности активов описана отдельно для каждого из них.

Ключевые слова: коммерческая организация, актив, ущерб, информационная безопасность, защита информации.

METHODOLOGY FOR DETERMINING THE VALUE OF PROTECTED ASSETS FOR THE AUDIT OF PROVIDING THE INFORMATION SECURITY OF A COMMERCIAL ORGANIZATION

O.M. Golembiovskaya, K.E. Shinakov, E.V. Kondrashova, A.P. Zholnerov

The article discusses the methodology associated with determining the value of assets for auditing information security of a commercial organization. In addition, an approach is proposed to predict the possible damage to the assets under consideration. It is advisable to apply the proposed methodology to the security services of the enterprise in order to identify the shortcomings of the protection system and implement various measures to neutralize or minimize the likelihood of possible threats. Determining the value of an organization's assets is an important stage of the audit. The main assets of a commercial organization from the point of view of ensuring information security are: an information system, a server, computers and other equipment for the work of employees, internal databases. The procedure for determining the value of assets is described separately for each of them.

Keywords: commercial organization, asset, damage, information security, information protection.

DOI 10.36622/VSTU.2021.24.3.010
УДК 004.056

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДВУХЭТАПНОЙ МОДЕЛИ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ СЕТЕВЫХ АВТОМАТИЗИРОВАННЫХ СТРУКТУР

А.И. Шеншин, Е.А. Шварцкопф, К.А. Разинкин

В последние годы отмечается стремительный рост количества атак на информационные системы и ресурсы с использованием вредоносного кода и контента. Наряду с этим, происходит непрерывное совершенствование функциональных возможностей вирусов, позволяющих скрывать своё присутствие в системе. К сожалению, существующий арсенал моделей эпидемических процессов не позволяет эффективно учитывать период скрытого распространения инфекции с последующим реагированием систем защиты при практическом моделировании сетевых эпидемий. В представленном исследовании проведён анализ существующего методического обеспечения в области сетевой эпидемиологии и предложено описание (включая научно-методическое обоснование) дискретной двухэтапной модели эпидемического процесса, призванной разрешить указанное противоречие, а также - разработана методика построения этой модели, включающая соответствующие аналитические выражения для параметров моделирования.

Ключевые слова: вредоносный код, вредоносный контент, сеть, эпидемический процесс, информационно-телекоммуникационные сети, двухэтапные модели, риск.

MATHEMATICAL PROVISION OF TWO-STAGE MODEL OF EPIDEMIC PROCESSES OF NETWORKED AUTOMATED STRUCTURES

A.I. Shenshin, E.A. Shvartskopf, K.A. Razinkin

In recent years there is a rapid increase of number of attacks on information systems and resources using malicious code and content. Along with this, continuous improvement of self-presence hiding functionality of malware are taking place. Unfortunately, existing arsenal of epidemic process models does not provide an ability to effectively take into account a latent spread period of infection and following reaction of protection systems in cases of practical modeling of network epidemics. In presented research was carried out an analysis of the existing methodological works in the field of network epidemiology and was proposed a description (including scientific-methodological justification) of a discrete two-stage epidemic process model, which is designed to resolve said contradiction, and a methodology for constructing this model was developed, including the corresponding analytical expressions for the modeling parameters.

Keywords: malicious code, malicious content, network, epidemic process, information and telecommunication networks, two-stage models, risk.

DOI 10.36622/VSTU.2021.24.3.011
УДК 004.056

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АНАЛИЗА ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СЦЕНАРИЕВ КОМПЬЮТЕРНЫХ АТАК

С.С. Куликов, Н.Н. Мурзинов

В данной статье представлено описание принципов построения и функционирования, а также некоторые архитектурные особенности специального программного обеспечения, которое может использоваться для анализа защищённости информационных систем на основе базы данных паттернов (шаблонов) компьютерных атак, характерных для определенных типов нарушителей и их групп. Задача анализа защищенности является важным этапом работ по защите информации как при формировании требований по защите информации, так и при оценке эффективности уже реализованных мер. Ввиду нетривиального, а в какой-то мере и даже творческого характера, решение данной задачи требует высокой квалификации от специалиста, значимых временных и материальных затрат. Вследствие это возникает объективная задача по автоматизации такой деятельности. В работе описана попытка решения указанной задачи на основе разработки программного обеспечения, использующего данные из открытых источников, обобщающих опыт и квалификацию специалистов информационной безопасности из разных стран.

Ключевые слова: анализ защищенности, информационная система, открытые данные.

DEVELOPMENT OF SOFTWARE TO ANALYZE THE SECURITY OF INFORMATION SYSTEMS BASED ON COMPUTER ATTACK PATTERNS

S.S. Kulikov, N.N. Murzinov

This article provides a description of the principles of construction and operation, as well as some architectural features of special software that can be used to analyze the security of information systems based on a database of patterns (patterns) of computer attacks typical for certain types of violators and their groups. The task of analyzing security is an important stage in information security work both in the formation of information security requirements and in assessing the effectiveness of measures already implemented. Due to the non-trivial, and to some extent even creative nature, the solution of this problem requires high qualifications from a specialist, significant time and material costs. As a result, an objective task arises to automate such activities. This paper describes an attempt to solve this problem on the basis of software development using data from open sources, summarizing the experience and qualifications of information security specialists from different countries.

Keywords: security analysis, information system, open data.