DOI 10.36622/VSTU.2022.25.1.001
УДК 004.056.57

СИСТЕМА МЕТОДОВ КАРТОГРАФИРОВАНИЯ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА

А.Л. Сердечный

Настоящая работа структурирует методологию построения и анализа информационных карт. Предложено подробное описание системы методов, необходимых для построения и анализа информационных карт. В качестве основных групп методов рассматриваются: методы подготовки данных для информационной карты (моделирование данных на основе источников, веб-скрапинг и др.), методы визуализации информационной карты (методы укладки графов, построение тепловой карты и др.), методы актуализации информационной карты (метод совмещения графов, метод трансформации ландшафта), традиционные картографические методы (графический оверлей, разметка областей карты и др.), сетевые методы (методы расчёта метрик графа, методы кластеризации графа и др.). Предлагаемая система методов является достаточной для проведения всесторонних картографических исследований защищаемого киберпространства, так и других сетевых структур, моделирующих предметную область. Также допускается расширение данной системы дополнительными методами, направленными на повышение эффективности процессов построения и анализа информационных карт.

Ключевые слова: метод, информационная карта, киберпространство, граф.

SYSTEM OF PROTECTED CYBERSPACE MAPPING METHODS

A.L. Serdechnyy

This paper structures a methodology for the construction and analysis of information maps. A detailed description of the system of methods required for the construction and analysis of information maps is offered. The main groups of methods considered are: data preparation methods for information map (source-based data modeling, web scraping, etc.), information map visualization methods (graph layout methods, heat map, etc.), information map updating methods (graph matching method, landscape transformation method), traditional cartographic methods (graphic overlay, map area markup, etc.), network methods (graph ranking, graph clustering etc.) The proposed system of methods is sufficient to conduct comprehensive mapping studies of the protected cyberspace, as well as other network structures modeling the subject area. It is also possible to extend this system with additional methods aimed at increasing the efficiency of information map construction and analysis processes.

Keywords: method, cyberspace, information map, graph.

DOI 10.36622/VSTU.2022.25.1.002
УДК 004.056

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В РФ

Ю.Ю. Громов, П.Ю. Пушкин, П.И. Карасев, А.Г. Иванов

В работе рассматривается понятие свободного программного обеспечения, его характерные черты, особенности, а также преимущества и недостатки. Описываются причины заинтересованности государственных органов в осуществлении политики, направленной на развитие свободного программного обеспечения вместо устоявшихся проприетарных средств. В хронологическом порядке приводятся распоряжения и приказы государственных органов, которые задают требования по реализации мероприятий, направленных на осуществление политики импортозамещения программного обеспечения в Российской Федерации, а также их результаты. Проводится статистический анализ использования некоторых программных продуктов, относящихся к свободному программному обеспечению. На основании данного исследования выдвигаются предположения о причинах установленной заинтересованности конечных пользователей в применении свободного программного обеспечения для ежедневных нужд. В завершении делается заключение о перспективах внедрения свободного программного обеспечения вместо имеющихся и используемых на данный момент проприетарных программных средств.

Ключевые слова: свободное программное обеспечение, импортозамещение, анализ, статистика.

PROBLEMS AND PROSPECTS OF IMPORT SUBSTITUTION OF SOFTWARE IN THE RUSSIAN FEDERATION

Y.Y. Gromov, P.Y. Pushkin, P.I. Karasev, A.G. Ivanov

The paper deals with the concept of free software, its characteristic features, features, as well as advantages and disadvantages. The reasons for the interest of government agencies in the implementation of policies aimed at the development of free software for the place of established proprietary tools are described. In chronological order, orders and orders of state bodies are given, which set the requirements for the implementation of measures aimed at implementing the software import substitution policy in the Russian Federation, as well as their results. A statistical analysis of the use of some software products related to free software is carried out. Based on this study, it is hypothesized about the reasons for the established interest of end users in the use of free software for daily needs. In the end, a conclusion is made about the prospects for introducing free software instead of the proprietary software that is currently available and used at the moment.

Keywords: free software, import substitution, analysis, statistics.

DOI 10.36622/VSTU.2022.25.1.003
УДК 004.056.57

СПОСОБЫ ПОСТРОЕНИЯ И АНАЛИЗА ИНФОРМАЦИОННЫХ КАРТ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА

А.Л. Сердечный

В статье рассматриваются типовые комбинации способов построения и анализа информационной карты. В частности, проиллюстрирована комбинация таких способов на примере библиометрических сетей. Рассмотрены особенности реализации способов построения и анализа информационных карт, определяемых их масштабом (крупным, средним и мелким), одним из которых является эффект совмещения несвязанных кластеров, обусловленный ошибками понижения размерности. Также показана специфика реализации способов, связанная с использованием модели данных на примере графа связей. Информационные карты по типу сущностей модели разделяются на объектные и субъектные. В свою очередь типы связей между сущностями определяют возможности отображения структурных и функциональных взаимодействий между субъектами и объектами. Вышеизложенное проиллюстрировано на примере графов терминов и связей публикаций и ключевых слов для учебной дисциплины «Компьютерные преступления». Рассмотренные комбинации способов построения и анализа информационных карт являются типовыми для проведения картографического анализа большинства сетевых структур и могут быть использованы в ходе решения широкого спектра задач в области обеспечения информационной безопасности и защиты информации.

Ключевые слова: способы, информационная карта, научная школа, граф, модель данных.

TECHNIQUES FOR CONSTRUCTING AND ANALYSIS OF PROTECTED CYBERSPACE INFORMATION MAPS

A.L. Serdechnyy

The article discusses typical combinations of techniques for building and analyzing an information card. In particular, a combination of such techniques is illustrated by the example of bibliometric networks. The features of the technique implementation for constructing and analyzing information maps determined by its scale (large, medium and small). One of the feature is an effect of combining unbound clusters, due to errors of a dimension lowering. Also shows the specifics of the implementation of techniques associated with using the data model, on the example of the bond graph. Information maps by type of entity of the model are divided into object and subject maps. In turn, the types of ties between entities determine the possibilities of displaying structural and functional interactions between the subjects and objects. The above is illustrated by the example of the graphs of terms and links of publications and keywords for the educational discipline "Computer crimes". The considered combinations of methods for building and analyzing information cards are typical for making a cartographic analysis of most network structures and can be used during solving a wide range of tasks in the field of information security and information protection

Keywords: techniques, information map, scientific school, graph, data model.

DOI 10.36622/VSTU.2022.25.1.004
УДК 004.931

РАСПОЗНАВАНИЕ ЛИЦ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ ПРИ ПОСТРОЕНИИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.Ю. Громов, П.И. Карасев, Ю.А. Губсков

Распознавание лиц - это процесс идентификации одного или нескольких людей на изображениях или видео. Это важная часть биометрических систем, систем безопасности и наблюдения, а также систем индексации изображений. В литературе были предложены различные методы распознавания лиц, такие как собственные векторы, методы, основанные на выделении признаков, скрытая модель Маркова и методы, основанные на нейронных сетях. Первые три метода в основном включают фазу извлечения или предварительной обработки объектов, тесно связанную с типом распознаваемого изображения. С другой стороны, технология нейронных сетей не требует конкретных данных о типе изображения, поэтому может быть применена к любому типу изображения и в то же время обеспечивает лучшую точность. В этой статье была предпринята попытка объединить технологии нейронной сети с нечеткой логикой. Экспериментальный результат показывает, что сочетание этих двух методов обеспечивает лучшую точность по сравнению с другими методами, упомянутыми выше.

Ключевые слова: распознавание лиц, нейронная сеть, нечеткая логика

FACE RECOGNITION USING NEURAL NETWORK TECHNOLOGIES IN THE CONSTRUCTION OF INFORMATION SECURITY SYSTEMS

Y.Y. Gromov, P.I. Karasev, Y.A. Gubskov

Face recognition is the process of identifying one or more people in images or videos. It is an important part of biometric systems, security and surveillance systems, and image indexing systems. Various face recognition methods have been proposed in the literature, such as: eigenvectors, feature-based methods, hidden Markov model, and neural network-based methods. The first three methods mainly include an object extraction or pre-processing phase, closely related to the type of image being recognized. On the other hand, neural network technology does not require specific data about the image type, so it can be applied to any type of image and at the same time provides better accuracy. In this article, an attempt was made to combine neural network technologies with fuzzy logic. The experimental result shows that the combination of these two methods provides better accuracy compared to the other methods mentioned above.

Keywords: face recognition, neural network, fuzzy logic.

DOI 10.36622/VSTU.2022.25.1.005
УДК 004.056.57

ПЕРСПЕКТИВЫ ПОСТРОЕНИЯ ГЕНЕРАЛЬНОЙ КАРТЫ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА

А.Л. Сердечный

В статье рассматривается представление генеральной карты киберпространства на его физическом, информационном и социальном уровнях. Применительно к физическому уровню обозначены ландшафты операторов, зон взаимодействия устройств интернета вещей, расположения киберфизических систем. В номенклатуру ландшафтов информационного уровня включены: данные о логических маршрутах с учетом различных сетевых протоколов; альтернативные протоколы, организующие работу обособленных виртуальных пространств; карты содержимого информационных ресурсов, онтологий и банков данных. На социальном уровне отмечается обилие объектов с множественными межслойными пересечениями. Рассматриваются также координаты объектов киберпространства через идентификаторы уровня, типового слоя, набора данных, алгоритма проецирования слоя, изображения объекта в рамках слоя. Слои кибепространства предлагается определять с учетом возможности масштабирования. Проекции слоев киберпространства позволяют рассматривать одни и те же объекты в различных вариантах расположения на плоскости или в трехмерном пространстве. Масштабирование слоев киберпространства позволяет организовывать направленную работу с большими данными. Вниманию читателя предлагаются многочисленные примеры, иллюстрирующие вышеизложенные методические рекомендации.

Ключевые слова: генеральная карта, уровни, идентификаторы, слои, объекты, масштабирование, проекции.

PROSPECTS FOR BUILDING THE GENERAL MAP OF PROTECTED CYBERSPACE MAPS

A.L. Serdechnyy

The article discusses the presentation of a general map of cyberspace at its physical, informational and social levels. With regard to the physical layer, the landscapes of operators, zones of interaction of IoT devices, and the location of cyber-physical systems are indicated. The nomenclature of information-level landscapes includes: data on logical routes, taking into account various network protocols; alternative protocols organizing the work of isolated virtual spaces; content maps of information resources, ontologies and data banks. At the social level, there is an abundance of objects with multiple interlayer intersections. The coordinates of objects in cyberspace are also considered through the identifiers of a level, a typical layer, a dataset, a layer projection algorithm, an object image within a layer. Cyberspace layers are proposed to be defined taking into account the scalability. Cyberspace layer projections allow viewing the same objects in different layouts on a plane or in three-dimensional space. Scaling the layers of cyberspace allows you to organize directed work with big data. The reader is offered numerous examples illustrating the above guidelines.

Keywords: general map, levels, identifiers, layers, objects, scaling, projections.

DOI 10.36622/VSTU.2022.25.1.006
УДК 378:004.056.57

СОЦИОТЕХНИЧЕСКОЕ ТЕСТИРОВАНИЕ В УСЛОВИЯХ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛИСТОВ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЭТАПЫ ПРОВЕДЕНИЯ И СЦЕНАРИИ АТАК

З.В. Семенова, Н.А. Моисеева, Е.В. Толкачева, Д.А. Бибик

В статье представлен анализ современного состояния проблемы атак на основе социальной инженерии. Рассматриваются методы и средства формирования иммунитета к атакам социальной инженерии вообще и фишинговым атакам, в частности. Проведен анализ современных подходов, отражающих основные этапы и сценарии проведения социотехнического тестирования, а также анализ терминологии в этой области. Обосновывается необходимость проведения социотехнических учений (Social Engineering Penetration Testing) для 100% студентов высших учебных заведений. Выявлены особенности учебного процесса, которые существенным образом влияют на подготовку и проведение социотехнического тестирования. Предложены техническая и программная инфраструктуры социотехнического тестирования. Подробно описаны пять сценариев, которые предлагается реализовать в рамках социотехнического тестирования. Кроме того, представлены ряд ограничений применения сценариев, совокупность созданных сервисов, обеспечивающих реализацию предложенных сценариев социотехнического тестирования и условия проведения подготовительных работ.

Ключевые слова: информационная безопасность, кибератака, атака социальной инженерии, социотехническое тестирование, тестирование на проникновение в социальную инженерию.

SOCIO-TECHNICAL TESTING UNDER FUTURE INFORMATION SECURITY SPECIALISTS' TRAINING: STAGES AND ATTACK SCENARIOS

Z.V. Semenova, N.A. Moiseeva, E.V. Tolkacheva, D.A. Bibik

The article presents the analysis of the current state of the problem of attacks based on social engineering. Methods and means of forming immunity to social engineering attacks in general and phishing attacks in particular are considered. The paper presents the analysis of modern approaches reflecting the main stages and scenarios of conducting socio-technical testing, as well as the analysis of terminology in this area. The necessity of Social Engineering Penetration Testing for 100% of higher educational institutions students is justified. The features of the educational process that significantly affect the preparation and conducting Social Engineering Penetration Testing are described. The technical and software infrastructure of socio-technical testing is proposed. Five scenarios that are suggested to be implemented within the framework of socio-technical testing are described in detail. In addition, a number of restrictions on the use of the described scenarios are presented. The description of the created services that ensure the implementation of the proposed scenarios of socio-technical testing and the conditions for conducting preparatory work is presented.

Keywords: Information Security, Cyberattack, Social Engineering Attack, Socio-technical Testing, Social Engineering Penetration Testing.

DOI 10.36622/VSTU.2022.25.1.007
УДК 004.056.57

КАРТОГРАФИРОВАНИЕ КИБЕРПРОСТРАНСТВА И ЗАЩИТА ИНФОРМАЦИИ

А.Г. Остапенко, А.Л. Сердечный, С.Д. Трубицын, Д.А. Нархов, В.Ю. Остапенко

В статье рассматривается обеспечение ситуационной осведомленности об угрозах безопасности информации и компьютерных атаках с использованием центров реагирования на инциденты и информационных карт, включая ситуационные центры управления кибербезопасностью. Вышеуказанная осведомленность иллюстрируется информационными картами APT-группировок, отражающими состав жертв и заинтересованных в них атаке строк; артефакты в коде вредоносного программного обеспечения; атрибуцию группировки на основании авторского стиля написания программных средств реализации компьютерных атак. В этой связи представлены общие планы информационных карт для разнообразных APT-группировок. При этом обсуждается противодействие киберпреступности с использованием информационных карт. Обсуждается анализ финансовых операций злоумышленников в виртуальном пространстве за счет использования криптовалют. На примерах Blockchain и Bitcoin-транзакций рассматривается определение принадлежности криптокошельков. С помощью графа связей иллюстрируются вышеупомянутые транзакции. Предлагается также анализ вредоносного программного обеспечения как инструмента кибератак. В этой связи рассматривается информационная карта связей способов реализации компьютерных атак и объектов воздействия, построенная на основании онтологии.

Ключевые слова: ситуационная осведомленность, информационная карта, кибербезопасность, криптовалюта, транзакции.

CYBERSPACE MAPPING AND INFORMATION PROTECTION

A.G. Ostapenko, A.L. Serdechnyy, S.D. Trubitsyn, D.A. Narkhov, V.Yu. Ostapenko

The article discusses the provision of situational awareness of information security threats and computer attacks using incident response centers and information maps, including situational cybersecurity control centers. The aforementioned awareness is illustrated by information maps of the ART groups, reflecting: the composition of the victims and those interested in them in the attack of strings; artifacts in the code of malicious software; attribution of a grouping based on the author's style of writing software for implementing computer attacks. In this regard, general plans of information cards for various ART groups are presented. At the same time, countering cybercrime using information cards is discussed. The analysis of financial transactions of cybercriminals in the virtual space through the use of cryptocurrencies is discussed. Using the examples of Blockchain and Bitcoin transactions, he considers the determination of the ownership of crypto wallets. With the help of a link graph, the above transactions are illustrated. Analysis of malware as a cyber attack tool is also proposed. In this regard, an information map of connections between methods of implementing computer attacks and objects of influence, built on the basis of an ontology, is considered.

Keywords: situational awareness, information map, cybersecurity, cryptocurrency, transactions.

DOI 10.36622/VSTU.2022.25.1.008
УДК 004.931

МЕТОДЫ ОБРАБОТКИ ДАННЫХ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ УМНОГО ВИДЕОНАБЛЮДЕНИЯ

Ю.Ю. Громов, П.И. Карасев, Ю.А. Губсков, В.О. Котюкова

В наше время видеонаблюдение является необходимой частью систем, которые повышают уровень обеспечения безопасности территории, имущества, персональных данных и в целом обеспечивает безопасность бизнеса. Распознавание образов на изображении с камер видеонаблюдения помогают автоматизировать данный процесс. Основная цель распознавания образов состоит в том, чтобы автоматически анализировать изображение с камер видеонаблюдения и извлекать из них необходимую информацию. Множество методов было разработано для большого количества систем, особенно для статического распознавания образов. Поскольку информация о многих процессах может быть не разобрана в течение продолжительного периода времени, для решения этой задачи может быть применен нечеткий подход. В этой работе будет реализован нечеткий подход к методам оптимизации в распознавании с изображения видеокамер. В нем будет показана нечеткая модель кластеризации данных и извлечения признаков, которая наилучшим образом подходит для процесса распознавания объектов на изображении, в условиях плохой освещенности или помех на изображении.

Ключевые слова: нечеткая кластеризация, видеонаблюдение, нечеткая логика

DATA PROCESSING METHODS IN INFORMATION SECURITY SYSTEMS IN ORGANIZING SMART VIDEO SURVEILLANCE

Y.Y. Gromov, P.I. Karasev, Y.A. Gubskov, V.O. Kotyukova

Today, video surveillance is a necessary part of systems that increase the level of security of the territory, property, personal data and, in general, ensures business security. Pattern recognition on the image from CCTV cameras helps to automate this process. The main goal of pattern recognition is to automatically analyze the image from CCTV cameras and extract the necessary information from them. Many methods have been developed for a large number of systems, especially for static pattern recognition. Since information about many processes may not be parsed for a long period of time, a fuzzy approach can be applied to solve this problem. In this work, a fuzzy approach to optimization methods in video camera image recognition will be implemented. It will show a fuzzy data clustering and feature extraction model that is best suited for the process of recognizing objects in an image, under conditions of poor lighting or noise in the image.

Keywords: fuzzy clustering, video surveillance, fuzzy logic.

DOI 10.36622/VSTU.2022.25.1.009
УДК 004.056.57

КАРТОГРАФИРОВАНИЕ КИБЕРПРОСТРАНСТВА И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Г. Остапенко, А.Л. Сердечный, С.Д. Трубицын, Д.А. Нархов, В.Ю. Остапенко

В статье приведены примеры задач обеспечения информационной безопасности, решаемых с использованием информационных карт. Исследуются элементы информационного противоборства в контекстах распространения информационной повестки, выгодной распространителю, и блокирования информационного влияния противника. В этой связи представлены сведения об информационной карте обмена контентом между крупными средствами массовой информации, а также демонстрируется сама карта данного обмена. В свете противодействия распространению деструктивного контента приведены сведения об информационной карте диффузии данного контента в сообществах единой тематики, а также сведения о способах реализации контент-атак, используемых APT-группировками. Разработанную информационную карту предлагается использовать для анализа динамики процесса распространения контентов внутри сообществ, в том числе и для расчета рисков диффузии деструктивного контента. Рассматривается также обеспечение информационно-психологической безопасности (в виртуальных средах) с помощью информационных карт. Для примера, анализу были подвержены музыкальные предпочтения. В этой связи построена информационная карта, основанная на данных сервиса «Яндекс.Музыка», а также определены профили музыкальных предпочтений.

Ключевые слова: информационная карта, сведения, контент, сообщества, предпочтения, безопасность.

CYBERSPACE MAPPING AND INFORMATION SECURITY

A.G. Ostapenko, A.L. Serdechnyy, S.D. Trubitsyn, D.A. Narkhov, V.Yu. Ostapenko

The article provides examples of information security tasks that can be solved using information cards. The article examines the elements of information warfare in the context of the dissemination of the information agenda, beneficial to the distributor, and blocking the information influence of the adversary. In this regard, information about the information card for the exchange of content between major media is presented, and the card of this exchange itself is also shown. In the light of countering the spread of destructive content, information is provided on the information map of the diffusion of this content in communities of a single topic, as well as information on the methods of implementing content attacks used by ART groups. The developed information map is proposed to be used to analyze the dynamics of the content distribution process within communities, including for calculating the risks of diffusion of destructive content. Providing informational and psychological security (in virtual environments) with the help of information cards is also considered. For example, musical preferences were analyzed. In this regard, an information map based on data from the Yandex.Music service has been drawn up, and profiles of musical preferences have been determined.

Keywords: information card, information, content, communities, preferences, security.

DOI 10.36622/VSTU.2022.25.1.010
УДК 004.056.55

ИСПОЛЬЗОВАНИЕ МЕТОДА АУТЕНТИЧНОГО ШИФРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ОБЛАЧНОГО ХРАНИЛИЩА ДАННЫХ

О.В. Трубиенко, В.В. Филинов, П.И. Карасев, Д.А. Головченко

Аутентичное шифрования (когда проводится одновременное выполнение функций шифрования и взаимозависимостей) предназначено для обеспечения конфиденциальности, контроля целостности и достоверности данных. Стороны, которые имеют общие ключи, могут организовать не только шифрованный обмен сообщениями, но и осуществлять контроль целостности путем добавления имитовставок до сообщения, что позволяет убеждаться в приеме достоверного сообщения. Аутентичное шифрование обеспечивает определенную функциональную нить: ключи могут обновляться в процессе обработки данных; есть возможность шифровать только отдельные части сообщения или чередовать шифрованные и открытые сообщения; имитовставки могут отсутствовать или, наоборот, случаться несколько раз. Преимущественно алгоритмы аутентичного шифрования строят на базе блочных криптосистем, некоторые из них симулируют классический подход, исключая использование двух ключей, другие являются оригинальными конструкциями.

Ключевые слова: шифрование, защищенность, облачное хранилище, аутентичное шифрование.

USING THE AUTHENTIC ENCRYPTION METHOD TO INCREASE THE SECURITY OF CLOUD DATA STORAGE

O.V. Trubienko, V.V. Filinov, P.I. Karasev, D.A. Golovchenko

Authentic encryption (the simultaneous execution of encryption functions and mutual dependencies is carried out) is designed to ensure confidentiality, control the integrity and reliability of data. The parties who have shared keys can organize not only an encrypted message exchange, but also carry out integrity control by adding imits before the message, which allows you to make sure that a reliable message is received. Authentic encryption provides a certain functional thread: keys can be updated during data processing; it is possible to encrypt only individual parts of the message or alternate encrypted and open messages; there may be no extensions or, conversely, occur several times. Mostly authentic encryption algorithms are built on the basis of block cryptosystems: some of them simulate the classical approach, excluding the use of two keys, others are original designs.

Keywords: encryption, security, cloud storage, authentic encryption.

DOI 10.36622/VSTU.2022.25.1.011
УДК 004.056

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫХ С АТАКАМИ НА ЦЕПИ ПОСТАВОК

С.С. Куликов, В.И. Белоножкин, Н.А. Юкин

В данной статье представлен анализ угроз информационной безопасности, связанных с атаками на цепи поставок, которые могут использоваться для нарушения информационной безопасности организации без прямых воздействий на ее информационно-технологическую инфраструктуру. В контексте информационной безопасности, атака на цепь поставки предполагает целенаправленные злоумышленные воздействия на активы поставщика с целью последующего нарушения информационной безопасности потребителя. Этот тип атак сегодня приобретает особую актуальность как наиболее эффективный среди всего множества угроз информационной безопасности ввиду принципиальных особенностей, существенно затрудняющих противодействие им: возможность злоумышленника по выбору наиболее незащищенного элемента для атаки, необходимость координации действий нескольких организационных структур для противодействия таким атакам, устранения последствий от их реализации и расследования их причин. Также приведен анализ научной, методической и технической литературы, описывающей сценарии известных атак на цепи поставок программного и аппаратного обеспечения.

Ключевые слова: угрозы информационной безопасности, цепи поставок, атаки на цепи поставок, риски информационной безопасности

ANALYSIS OF INFORMATION SECURITY THREATS, ASSOCIATED WITH SUPPLY CHAIN ATTACKS

S.S. Kulikov, V.I. Belonozhkin, N.A. Yuyukin

This article presents an analysis of information security threats associated with attacks on the supply chain, which can be used to violate the information security of an organization without direct impacts on its information technology infrastructure. In the context of information security, an attack on the supply chain involves targeted malicious impacts on the supplier's assets with the aim of further violating the consumer's information security. This type of attacks is becoming particularly relevant today as the most effective among all the many threats to information security due to the fundamental features that significantly complicate countering them: the possibility of choosing the most unprotected element of the chain for an attack, the need to coordinate the actions of several organizational structures to counter such attacks, eliminate the consequences of their implementation and investigate their causes. The analysis of scientific, methodological and technical literature describing scenarios of known attacks on the supply chain of software and hardware is also given.

Keywords: information security threats, supply chains, supply chain attacks, information security risks.

DOI 10.36622/VSTU.2022.25.1.012
УДК 004.942

МОДЕЛЬ АДАПТИВНОГО КОНТРОЛЯ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК

С.А. Коноваленко

В целях повышения эффективности системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) в статье разработана модель адаптивного контроля ее структурных элементов. Проведена последовательная многоэтапная процедура адаптации исследуемого процесса, обеспечивающая возможность контроля гетерогенной СОПКА, эксплуатируемой в условиях часто появляющихся фактов неустойчивых сетевых взаимодействий с системой адаптивного контроля, с минимальным уровнем расхода операционных ресурсов всех видов. Определено множество функций, реализуемых системой адаптивного контроля гетерогенной СОПКА и позволяющих нейтрализовать угрозы безопасности информации, связанные с подменой ее структурных элементов, обеспечить контроль ее мобильных структурных элементов, снизить ресурсоемкость, возможную избыточность и меру неопределенности результатов адаптивного контроля, а также повысить их достоверность и информативность. Разработана структурно-функциональная модель адаптивного контроля гетерогенной СОПКА, описывающая итерационный процесс своего функционирования и облегчающая возможность практической реализации предлагаемых научно-технических решений, позволяющих достичь синергетического эффекта посредством задания последовательности реализации существующих методов контроля с учетом различных условий эксплуатации гетерогенной СОПКА.

Ключевые слова: адаптивный контроль, система обнаружения, предупреждения и ликвидации последствий компьютерных атак.

MODEL OF ADAPTIVE CONTROL OF A SYSTEM OF DETECTING, PREVENTING AND ELIMINATING THE CONSEQUENCES OF COMPUTER ATTACKS

S.A. Konovalenko

In order to improve the efficiency of the system for detecting, preventing and eliminating the consequences of computer attacks (SOPKA), the article has developed a model for adaptive control of its structural elements. A sequential multi-stage procedure for adapting the process under study has been carried out, which provides the ability to control a heterogeneous SOPKA, operated in conditions of frequent occurrences of unstable network interactions with the adaptive control system, with a minimum level of consumption of all types of operating resources. The set of functions implemented by the adaptive control system of heterogeneous SOPKA and allowing to neutralize threats to information security associated with the substitution of its structural elements, to ensure control of its mobile structural elements, to reduce resource consumption, possible redundancy and uncertainty of the results of adaptive control, and also to increase their reliability and information content have been determined. A structural and functional model of adaptive control of a heterogeneous SOPKA has been developed, which describes the iterative process of its functioning and facilitates the possibility of practical implementation of the proposed scientific and technical solutions that allowing to achieve a synergistic effect by setting a sequence for the implementation of existing control methods, taking into account various operating conditions of a heterogeneous SOPKA.

Key words: adaptive control, a system of detecting, preventing and eliminating the consequences of computer attacks.

DOI 10.36622/VSTU.2022.25.1.013
УДК 004.056

СПЕЦИАЛИТЕТ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»: КРАТКИЕ НАУЧНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ КУРСОВОГО ЗАДАНИЯ ДЛЯ ДИСЦИПЛИНЫ «ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ»

К.А. Разинкин, В.Н. Кострова, В.М. Питолин, Н.М. Лантюхов, Д.А. Нархов

Рассматриваются научно-методические рекомендации, полезные для первокурсников в рамках выполнения ими индивидуальных курсовых заданий по дисциплине «Введение в специальность». Считая исключительно полезным освоение студентами методологии риск-мониторинга популярных интернет-ресурсов, авторы предлагают подходы к постановке соответствующих задач, способов их решения и структуризации курсовой работы. Ориентация на актуальные программные средства открывает перспективы для каждого первокурсника и выпускающей кафедры в целом получения емких, актуальных и научно-технически значимых результатов о социо-информационных рисках, порождаемых в интернет-ресурсах при распространении и восприятии контентов с признаками деструктивности. Работа ориентирована на специальности группы «Информационная безопасность». Предложения, сформулированные в ней, учитывают опыт подготовки и защиты курсовых работ по вышеуказанным специальностям, сложившийся в Воронежском государственном техническом университете. Стремительное нарастание множества и опасности информационных рисков, порождаемых революционной цифровой трансформацией личности, общества и государства, обуславливает практическую актуальность научно-методических рекомендаций настоящей работы для студентов направления «Информационная безопасность».

Ключевые слова: контент, риск, угрозы, аналитическая оценка, объект и предмет исследования, противоречия, результаты.

SPECIALTY "INFORMATION SECURITY": BRIEF SCIENTIFIC AND METHODOLOGICAL RECOMMENDATIONS FOR THE IMPLEMENTATION OF THE COURSE ASSIGNMENT FOR THE DISCIPLINE "INTRODUCTION TO THE SPECIALTY"

K.A. Razinkin, V.N. Kostrova, V.M. Pitolin, N.M. Lantyukhov, D.A. Narhov

Scientific and methodological recommendations useful for first-year students in the framework of their individual course assignments in the discipline "Introduction to the specialty" are considered. Considering it extremely useful for students to master the methodology of risk monitoring of popular Internet resources, the authors propose approaches to setting appropriate tasks, ways to solve them and structuring course work. Orientation to current software tools opens up prospects for each freshman and the graduating department as a whole to obtain capacious, relevant and scientifically and technically significant results on socio-informational risks generated in Internet resources when distributing and perceiving content with signs of destructiveness. The work is focused on the specialties of the Information Security group. The proposals formulated in it take into account the experience of preparing and defending term papers in the above-mentioned specialties that has developed at the Voronezh State Technical University. The rapid increase in the multitude and danger of information risks generated by the revolutionary digital transformation of the individual, society and the state determines the practical relevance of the scientific and methodological recommendations of this work for students of the direction "Information Security".

Keywords: content, risk, threats, analytical assessment, object and subject of research, contradictions, results.