DOI 10.36622/VSTU.2022.25.2.001
УДК 004.41 : 004.45

РАСШИРЕННАЯ МОДЕЛЬ ОТКРЫТЫХ СИСТЕМ (ЧАСТЬ 1)

К.А. Бугайский, Д.С. Бирин, Б.О. Дерябин, С.О. Цепенда

В первой части статьи на основании информации, изложенной в прилагаемом списке литературы показано, что основные принципы референсной модели открытых систем OSR/RM по-прежнему актуальны несмотря на «закрытие» данной модели и отказ от ее развития. Это дает основания предложить, что на основе принципов OSE/RM могут быть описаны современные информационные системы. В рамках этой гипотезы предложено расширение модели OSE/RM за счет добавления двух уровней: данных и пользователей. Для учета современных тенденций построения вычислительных систем каждый уровень рассматривается как набор уровней абстракций, которые могут группироваться в подсистемы. В рамках модели, кроме плоскостей, слоев и уровней абстракции определены основные компоненты: программные сущности, информационные единицы, конфигурации и механизмы коммуникаций.

Ключевые слова: открытые системы, информационная безопасность, модель, информационная система.

EXTENDED MODEL OF OPEN SYSTEMS (PART 1)

K.A. Bugayskiy, D.S. Birin, B.O. Deryabin, S.O. Tsependa

In the first part of the article, based on the information provided in the attached list of references, it is shown that the basic principles of the reference model of open OSR/RM systems are still relevant despite the "closure" of this model and the rejection of its development. This gives grounds to suggest that modern information systems can be described based on the principles of OSE/RM. Within the framework of this hypothesis, an extension of the OSI/RM model is proposed by adding two levels: data and users. To take into account current trends in the construction of computing systems, each level is considered as a set of abstraction levels that can be grouped into subsystems. Within the framework of the model, in addition to planes, layers and levels of abstraction, the main components are defined: program entities, information units, configurations and communication mechanisms.

Key words: open systems, information security, model, information system.

DOI 10.36622/VSTU.2022.25.2.002
УДК 004.02 : 004.05

МЕТОДЫ СНИЖЕНИЯ ШУМОВЫХ ФАКТОРОВ ПРИ ВЫЯВЛЕНИИ КОНТЕНТА ЭКСТРЕМИСТСКОГО ХАРАКТЕРА В СОЦИАЛЬНЫХ МЕДИА

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

Цель исследования состоит в поиске методов снижения влияния шумовых эффектов при выявлении текстового контента экстремистского характера в социальных медиа. Осуществлен обзор методов, применяемых для выявления экстремистского контента, проанализированы их преимущества и недостатки. Сформирован экспериментальный текстовый корпус, моделирующий структуру реальных текстовых данных из социальных медиа и содержащий контент экстремистского характера о радикальном исламе. Описан процесс предобработки корпуса. Проанализированы методы классификации текста. Представлена работа моделей-трансформеров на примере трансформера BERT. Разработаны архитектуры классификаторов на основе BERT, используя различные методы многоклассовой и бинарной классификации. Проведены эксперименты по выявлению и классификации текстовых данных, содержащих экстремистский контент. Оценена точность и F-мера классификаторов в каждом эксперименте, обоснован выбор наиболее качественного классификатора для снижения шумовых факторов при выявлении контента экстремистского характера. Результаты работы классификатора на основе BERT превосходят результаты использования глубинных нейронных сетей (GRU, LSTM, CNN). Полученную модель классификатора и подход к снижению влияния шумовых факторов целесообразно применять при разработке систем мониторинга и выявления деструктивной информации в социальных медиа.

Ключевые слова: снижение шума, текстовый контент, экстремизм, социальные медиа, трансформер BERT, глубокое обучение, классификация.

METHODS OF REDUCING NOISE FACTORS IN THE PROCESS OF IDENTIFICATION EXTREMIST CONTENT IN SOCIAL MEDIA

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

The aim of the study is to find methods to reduce the impact of noise effects when identifying extremist text content in social media. A review of the methods used to identify extremist content is carried out, their advantages and disadvantages are analyzed. An experimental text corpus has been formed that simulates the structure of real text data from social media and contains extremist content about radical Islam. The process of preprocessing the case is described. The methods of text classification are analyzed. The work of transformer models is presented on the example of the BERT transformer. BERT-based classifier architectures have been developed using various methods of multiclass and binary classification. Experiments were conducted to identify and classify text data containing extremist content. The results of the BERT-based classifier are superior to the results of using deep neural networks (GRU, LSTM, CNN). The resulting classifier model and approach to reducing the influence of noise factors should be used when developing monitoring systems and identifying destructive information in social media

Keywords: noise reduction, text content, extremism, social media, transformer BERT, deep learning, classification.

DOI 10.36622/VSTU.2022.25.2.003
УДК 004.02 : 004.05

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ И АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

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

На сегодняшний день риски информационной безопасности являются большой угрозой для различных организаций. Защита информации становится одной из самых главных задач. В данной статье описывается анализ рисков и оценка эффективности защиты информационной системы и ее безопасности организации с целью предупреждения и оценки последствий угроз на систему. В наше время эта тема актуальная в силу того, что инциденты хищения информации, в целях нанесения вреда активам организации, достаточно часто происходят. В интересах каждой организации защищать активы от различных угроз, обеспечивая тем самым сохранность своим информационным ресурсам. В данной статье описаны проблемы сохранения свойств надёжности и эффективности защиты информационных систем, от угроз, которые могут негативно повлиять на работоспособность системы.

Ключевые слова: информационная безопасность, анализ рисков, оценка системы защиты, защита информации, эффективность защиты.

EVALUATION OF THE EFFECTIVENESS OF INFORMATION SECURITY SYSTEMS AND ANALYSIS OF INFORMATION SECURITY RISKS IN THE ORGANIZATION

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

Today, information security risks are a big threat to various organizations. Information protection is becoming one of the most important tasks. This article describes the risk analysis and evaluation of the effectiveness of the protection of the information system and its security of the organization in order to prevent and assess the consequences of threats to the system. Nowadays, this topic is relevant due to the fact that incidents of information theft, in order to harm the assets of the organization, quite often occur. It is in the interests of each organization to protect assets from various threats, thereby ensuring the safety of its information resources. This article describes the problems of preserving the properties of reliability and effectiveness of protecting information systems from threats that can negatively affect the performance of the system.

Keywords: information security, risk analysis, security system assessment, information security, protection efficiency.

DOI 10.36622/VSTU.2022.25.2.004
УДК 001.89 : 004.77

СПЕЦИАЛИТЕТ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»: КРАТКИЕ НАУЧНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПОДГОТОВКИ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

К.А. Разинкин, В.Н. Кострова, В.М. Питолин, Е.С. Соколова, Д.А. Нархов, А.Е. Прохорова

В статье описаны основные научно-методические рекомендации для подготовки выпускных квалификационных работ. Озвучена основная терминология, которая применяется в ходе дипломного проектирования и особенности классифицированного дерева, способствующего фундаментальному анализу угроз и рисков. Перечислены (в контексте исследования) пункты, основной мыслью которых является недопустимость использования информации, не имеющей под собой достаточно мощную теоретическую и доказательную базу. Прописаны рекомендации по подготовке выпускной квалификационной работы. Работа ориентирована на специальности «Информационная безопасность телекоммуникационных систем», «Информационная безопасность автоматизированных систем» и «Компьютерная безопасность». Предложения, сформулированные в ней, учитывают опыт подготовки и защиты ВКР 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 дипломников, их руководителей и выпускников кафедр специалитета «Информационная безопасность».

Ключевые слова: риск, угрозы, выпускная квалификационная работа, аналитическая оценка, объект и предмет исследования, противоречия, результаты.

SPECIALTY "INFORMATION SECURITY": BRIEF SCIENTIFIC AND METHODOLOGICAL RECOMMENDATIONS FOR THE PREPARATION OF FINAL QUALIFYING WORKS

K.A. Razinkin, V.N. Kostrova, V.M. Pitolin, E.S. Sokolova, D. A. Narhov, A.E. Prokhorova

The article describes the main scientific and methodological recommendations for the preparation of final qualifying papers. The basic terminology that is used during the diploma design and the features of the classified tree that contributes to the fundamental analysis of threats and risks are announced. The points are listed (in the context of the study), the main idea of which is the inadmissibility of using information that does not have a sufficiently powerful theoretical and evidence base. Recommendations for the preparation of the final qualifying work are prescribed. The work is focused on the specialties "Information security of telecommunication systems", "Information security of automated systems" and "Computer security". The proposals formulated in it take into account the experience of preparing and defending the final qualifying work in the above specialties, which 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 graduate students, their supervisors and graduates of the departments of the specialty "Information Security".

Keywords: risk, threats, final qualifying work, analytical assessment, object and subject of research, contradictions, results.

DOI 10.36622/VSTU.2022.25.2.005
УДК 004.02 : 004.05

ПОДХОДЫ К ОБНАРУЖЕНИЮ СОЦИАЛЬНЫХ ИНТЕРНЕТ-БОТОВ

А.О. Логинова

В данной статье представлен обзор подходов к обнаружению социальных интернет-ботов. Рассматриваются методики, основанные на выявлении автоматических или автоматизированных социальных акторов по следующим группам признаков: метаданные контролируемого ботом аккаунта, активность аккаунта, - также рассматриваются подходы к обнаружению ботов по совокупности признаков, в основе которых заложено машинное обучение (искусственный интеллект). Представленный обзор позволит выявить преимущества и недостатки существующих на сегодняшний день подходов к обнаружению социальных ботов, оценить возможность использования конкретного подхода в проектировании системы обнаружения ботов для определённого интернет-средства массовой коммуникации, оценить перспективы развития производства готовых отечественных решений по обнаружению социальных ботов. Статья подготовлена при поддержке Министерства науки и высшего образования Российской Федерации в рамках выполнения государственного задания в сфере науки № FSFU-2020-0020.

Ключевые слова: социальные интернет-боты, методика обнаружения ботов, информационно-психологическая безопасность, интернет-средства массовой коммуникации.

APPROACHES TO DETECTING SOCIAL INTERNET BOTS

A.O. Loginova

This article provides an overview of existing approaches to detecting social Internet bots. The methods based on identification of automatic or automated social actors by the following groups of signs: metadata of an account controlled by a bot, account activity; approaches to detecting bots by a set of signs based on machine learning (artificial intelligence) are also considered. This review reveals advantages and disadvantages of existing approaches to social bots detection, promotes a possibility to assess using a specific approach to design a bot detection system for a certain social net, a possibility to assess prospects for the development of production of solutions for social bots detection.

Keywords: social bots, methods of detecting bots, information-psychological security, Internet mass media.

DOI 10.36622/VSTU.2022.25.2.006
УДК 004.02 : 004.05

ИНСТРУМЕНТАЛЬНЫЙ ПОДХОД К ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.А. Маслова

Оценка рисков в информационной безопасности, как и в любой области является непрерывным процессом, который необходимо постоянно мониторить, видоизменять, усовершенствовать, так как быстро растущий и постоянно видоизменяющийся информационный поток, появляющиеся новые негативные факторы, а также внутренние и внешние контексты с новыми угрозами могут внести большие потери для предприятий. В условиях постоянных изменений в экономической сфере, необходимо своевременно реагировать на появляющиеся негативные тенденции и оперативно принимать соответствующие меры по их исправлению, т.е. управлять возможными рисками в данной области [1]. Необходимо создавать новые программы, которые будут соответствовать современным требованиям, законодательной базе и быть гибкими к постоянным изменениям во времени и новым появляющимся факторам, рискам и уязвимостям. Также они должны быстро и легко видоизменяться и иметь редактируемую базу данных. В данной статье будет рассмотрена значимость удаленной работы, статистика и приведено описание одного из блоков разрабатывающейся программы для оценки рисков информационной безопасности, которая содержит большую базу входных и выходных DataSet существующих методик.

Ключевые слова: информационная безопасность, риски, выходные данные, DataSet, удаленная работа.

INSTRUMENTAL APPROACH TO INFORMATION SECURITY RISK ASSESSMENT

M.A. Maslova

Risk assessment in information security, as in any field, is a continuous process that needs to be constantly monitored, modified, improved, since the rapidly growing and constantly changing information flow, emerging new negative factors, as well as internal and external contexts with new threats can cause great losses for enterprises. In the conditions of constant changes in the economic sphere, it is necessary to respond in a timely manner to emerging negative trends and promptly take appropriate measures to correct them, i.e. to manage possible risks in this area [1]. It is necessary to create new programs that will meet modern requirements, the legislative framework and be flexible to constant changes over time and new emerging factors, risks and vulnerabilities. They should also be modified quickly and easily and have an editable database. This article will consider the importance of remote work, statistics and a description of one of the blocks of the program being developed for assessing information security risks, which contains a large database of input and output datasets of existing techniques.

Key words: information security, risks, input data, output data, DataSet, remote work.

DOI 10.36622/VSTU.2022.25.2.007
УДК 004.8 : 04.077

КОМПЛЕКСНЫЙ АНАЛИЗ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.А. Ермаков, А.А. Болгов, Ю.А. Гусарева

В работе проводится комплексный анализ систем Интернета вещей с точки зрения их многоуровневой архитектуры, а также отмечены их ключевые характеристики и основные области и виды применения. Детально анализируются этапы создания и развития неоднородных сетей Интернета вещей. Проведен анализ статистики и прогнозов развития предмета исследования. Приведено описание соответствующих уровней модели взаимодействия открытых систем применительно к системам Интернета вещей. Сформирован набор общих характеристик, а также отличительных особенностей для систем Интернета вещей. Проанализированы наиболее распространённые области применения устройств Интернета вещей. Сформированы требования к безопасности на каждом уровне архитектуры систем, построенных на базе Интернета вещей. Проведен детальный анализ актуальных для решения проблем в области обеспечения информационной безопасности систем Интернета вещей.

Ключевые слова: интернет вещей, неоднородность, сеть, конфиденциальность, аутентификация, целостность, доступность.

COMPREHENSIVE ANALYSIS OF INTERNET OF THINGS SYSTEMS TO IDENTIFY VULNERABILITIES IN THE CONTEXT OF INFORMATION SECURITY

S.A. Ermakov, A.A. Bolgov, Ju.A. Gusareva

The paper provides a comprehensive analysis of the Internet of Things systems from the point of view of their multilevel architecture, as well as their key characteristics and main areas and application. The stages of creation and development of heterogeneous Internet of Things networks are analyzed in detail. The analysis of statistics and forecasts of the development of the subject of research is carried out, the description of the corresponding levels of the open systems interaction model in relation to the Internet of Things systems is given. A set of common characteristics, as well as distinctive features for the Internet of Things systems, has been formed. The most common applications of Internet of Things devices are analyzed. Security requirements have been formed at each level of the architecture of systems built on the basis of the Internet of Things. A detailed analysis of the problems relevant to solving in the field of information security of Internet of Things systems has been carried out.

Keywords: Internet of Things, heterogeneity, network, confidentiality, authentication, integrity, availability.

DOI 10.36622/VSTU.2022.25.2.008
УДК 004.8 : 04.077

ОБЗОР СУЩЕСТВУЮЩИХ ПРОЦЕДУР КОНТРОЛЯ ДОСТУПА В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.А. Болгов

Работа посвящена обзору существующих подходов к реализации контроля доступа, произведен анализ известных процедур контроля доступа и выполнено их сравнение применительно к обеспечению безопасности систем Интернета вещей. Подробно рассмотрены три способа реализации контроля доступа в системах Интернета вещей. Проведен анализ и сравнение статических и динамических процедур контроля доступа. Проанализированы наиболее распространённые процедуры контроля доступа. Рассмотрена процедура контроля доступа по критерию допустимости оценки риска безопасности авторизуемого объекта. Проведен анализ существующих процедур-аналогов для контроля доступа по критерию величины риска. Описаны основные параметры оценки риска для процедуры контроля доступа. Выделены преимущества и недостатки известных процедур и методик контроля доступа в контексте безопасности систем Интернета вещей.

Ключевые слова: контроль доступа, интернет вещей, конфиденциальность, аутентификация, целостность, доступность, риск, параметры риска, безопасность.

OVERVIEW OF EXISTING ACCESS CONTROL PROCEDURES IN THE CONTEXT OF ENSURING THE SECURITY OF INTERNET OF THINGS SYSTEMS

S.A. Ermakov, A.A. Bolgov

The work is devoted to the review of existing approaches to the implementation of access control, the analysis of known access control procedures and their comparison in relation to the security of Internet of Things systems. Three ways of implementing access control in Internet of Things systems are considered in detail. Static and dynamic access control procedures are analyzed and compared. The most common access control procedures are analyzed. The procedure of access control according to the criterion of the admissibility of the assessment of the security risk of the authorized object is considered. The analysis of existing analogous procedures for access control according to the criterion of risk magnitude is carried out. The main risk assessment parameters for the access control procedure are described. The advantages and disadvantages of well-known access control procedures and techniques in the context of the security of Internet of Things systems are highlighted.

Keywords: access control, Internet of Things, confidentiality, authentication, integrity, availability, risk, risk factors, security.

DOI 10.36622/VSTU.2022.25.2.009
УДК 510.6

НЕЧЕТКАЯ ЛОГИКА НА ОСНОВЕ ЭКСПЕРТНЫХ ОЦЕНОК КАК АЛЬТЕРНАТИВНЫЙ ИНСТРУМЕНТ ДЛЯ ОЦЕНКИ РИСКА В УСЛОВИЯ НЕОПРЕДЕЛЕННОСТИ

С.А. Ермаков, А.А. Болгов, А.Г. Чурсин

В работе рассматривается теория нечеткой логики на основе экспертных оценок. Проведен анализ теории нечетких множеств и сравнение с булевой логикой. Подробно изучены этапы фазификации, функций принадлежности, нечеткие правила, агрегация правил, дефазификация. Детально рассмотрены различные функции принадлежности применительно к теории нечетких множеств. Проанализированы приложения, в которых используется система нечеткой логики. Рассмотрены экспертные оценки, какими они бывают и от чего зависят. Выделены основные критерии для выбора эксперта из числа кандидатов. Выявлены особенности проведения собеседования с экспертами. Рассмотрены этапы получения экспертных оценок. Приведена сравнительная таблица методов сбора экспертных оценок. В заключении работы, сделан вывод о том, что система нечеткой логики на основе экспертной оценки является мощным инструментов в анализе рисков.

Ключевые слова: нечеткая логика, риск, количественная оценка, качественная оценка, функция принадлежности, безопасность.

FUZZY LOGIC BASED ON EXPERT ASSESSMENTS AS AN ALTERNATIVE TOOL FOR RISK ASSESSMENT IN CONDITIONS OF UNCERTAINTY

A.A. Bolgov, S.A. Ermakov, A.G. Chursin

The paper considers the theory of fuzzy logic based on expert assessments. The theory of fuzzy sets is analyzed and compared with Boolean logic. The stages of fuzzification, membership functions, fuzzy rules, rule aggregation, and defuzzification are studied in detail. Various membership functions are considered in detail in relation to the theory of fuzzy sets. The applications in which the fuzzy logic system is used are analyzed. Expert assessments are considered, what they are and what they depend on. The main criteria for selecting an expert from among the candidates are highlighted. The peculiarities of conducting interviews with experts are revealed. The stages of obtaining expert assessments are considered. A comparative table of methods for collecting expert assessments is given. In conclusion, it is concluded that the fuzzy logic system based on expert evaluation is a powerful tool in risk analysis.

Keywords: fuzzy logic, risk, quantitative assessment, qualitative assessment, membership function, security.

DOI 10.36622/VSTU.2022.25.2.010
УДК 004.8 : 04.077

ОБЗОР МЕТОДОВ ДЛЯ ПОСТРОЕНИЯ РИСК-ОРИЕНТИРОВАННОЙ МОДЕЛИ КОНТРОЛЯ ДОСТУПА В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.А. Болгов

В работе рассматривается понятие риска безопасности и способы его оценки. Проводится подробный обзор методов количественной и качественной оценки рисков и анализ их преимуществ и недостатков. Проведен детальный анализ применений методов оценки рисков в различных риск-ориентированных моделях контроля доступа, с выделением их преимуществ и недостатков. Приведены результаты сравнительного анализа преимуществ и ограничений применимости различных методов оценки риска. Рассмотрен подход на основе нечеткой логики на основе экспертных оценок. На основании проведенного анализа и результатов сравнения выбран метод нечеткой логики с экспертным оценками в качестве подходящего метода для реализации риск-ориентированной модели контроля доступа для систем на построенных на базе технологии Интернета Вещей.

Ключевые слова: контроль доступа, интернет вещей, нечеткая логика, оценка риска, количественная оценка, качественная оценка, риск, безопасность.

OVERVIEW OF METHODS FOR BUILDING A RISK-BASED ACCESS CONTROL MODEL IN INTERNET OF THINGS SYSTEMS

S.A. Ermakov, A.A. Bolgov

The paper discusses the concept of security risk and ways to assess it. A detailed review of methods of quantitative and qualitative risk assessment and analysis of their advantages and disadvantages is carried out. A detailed analysis of the applications of risk assessment methods in various risk-oriented access control models has been carried out, highlighting their advantages and disadvantages. The results of a comparative analysis of the advantages and limitations of the applicability of various risk assessment methods are presented. An approach based on fuzzy logic based on expert assessments is considered. Based on the analysis and comparison results, the fuzzy logic method with expert assessments was chosen as a suitable method for implementing a risk-based access control model for systems based on Internet of Things technology.

Keywords: access control, Internet of Things, fuzzy logic, risk assessment, quantitative assessment, qualitative assessment, risk, security.

DOI 10.36622/VSTU.2022.25.2.011
УДК 004.8 : 04.077

ОСНОВАННАЯ НА РИСКАХ АДАПТИВНАЯ ПРОЦЕДУРА КОНТРОЛЯ ДОСТУПА ДЛЯ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.А. Болгов

В работе предложена адаптивная процедура контроля доступа на основе рисков для системы Интернета вещей. Выявлены ограничения существующих статических процедур контроля доступа применительно к системам Интернета вещей. Определена необходимость использования динамической процедуры контроля доступа, основанной на рисках. В работе проанализированы существующие на сегодняшний день проблемы в данном направлении. Сформулированы задачи и методы для решения выявленных при анализе различных источников проблем. Предложена адаптивная процедура контроля доступа, основанная на рисках. Подробно описаны ее основные элементы и представлена блок-схема работы алгоритма этой процедуры. Представлены методы исследования, которые необходимо использовать для решения поставленных задач исследования. В заключении, представлено краткое изложение основных результатов, полученных в данной статье.

Ключевые слова: нечеткая логика, риск, количественная оценка, качественная оценка, оценка риска, экспертная оценка.

RISK-BASED ADAPTIVE ACCESS CONTROL PROCEDURE FOR INTERNET OF THINGS SYSTEMS

S.A. Ermakov, A.A. Bolgov

The paper proposes an adaptive access control procedure based on risks for the Internet of Things system. The limitations of the existing static access control procedures in relation to the Internet of Things systems are revealed. The necessity of using a dynamic access control procedure based on risks is determined. The paper analyzes the current problems in this direction. The tasks and methods for solving the problems identified in the analysis of various sources are formulated. An adaptive access control procedure based on risks is proposed. Its main elements are described in detail and a flowchart of the algorithm of this procedure is presented. The research methods that need to be used to solve the research tasks are presented. In conclusion, a summary of the main results obtained in this article is presented.

Keywords: fuzzy logic, risk, quantitative assessment, qualitative assessment, risk assessment, expert assessment.

DOI 10.36622/VSTU.2022.25.2.012
УДК 004.72

ПОДХОД К ОРГАНИЗАЦИИ ЕДИНОГО ЦЕНТРА МОНИТОРИНГА С СОХРАНЕНИЕМ СВОЙСТВА ФИЗИЧЕСКОЙ ИЗОЛЯЦИИ СЕГМЕНТОВ ДЛЯ ИЗНАЧАЛЬНО НЕПЕРЕСЕКАЮЩИХСЯ СЕТЕЙ

Ю.Ю. Громов, П.И. Карасев, Ю.Д. Забалуева, Д.Д. Маланьин

На сегодняшний день задача контроля функционирования инфраструктуры является актуальной для многих организаций. Осуществление централизованного контроля позволяет улучшить показатели реагирования на инциденты и снизить потенциальный ущерб. Задача сохранения безопасности инфраструктуры является важным аспектом, которых необходимо учитывать при внедрении новых элементов в функционирующую информационную систему. В наше время эта тема имеет большую значимость в силу постоянно развивающихся способов атак на инфраструктуру организации. В данной статье описаны методы сохранения уровня безопасности инфраструктуры на прежнем уровне после внедрения единого центра мониторинга, использование которого позволяет ускорить реагирование на инциденты.

Ключевые слова: информационная безопасность, система мониторинга, непересекающиеся сети, однонаправленный канал передачи.

AN APPROACH TO ORGANIZING A SINGLE MONITORING CENTER WHILE MAINTAINING THE PROPERTY OF PHYSICAL ISOLATION OF SEGMENTS FOR INITIALLY NON-OVERLAPPING NETWORKS

Y.Y. Gromov, P.I. Karasev, Y.D. Zabalueva, D.D. Malanin

Today, the task of monitoring the functioning of the infrastructure is relevant for many organizations. Implementation of centralized control allows you to improve incident response rates and reduce potential damage. The task of maintaining infrastructure security is an important aspect that must be taken into account when introducing new elements into a functioning information system. In our time, this topic is of great importance due to the constantly evolving methods of attacks on the infrastructure of the organization. This article describes methods for maintaining the security level of the infrastructure at the same level after the implementation of a single monitoring center, the use of which allows you to accelerate incident response.

Keywords: information security, monitoring system, non-overlapping networks, unidirectional transmission channel.

DOI 10.36622/VSTU.2022.25.2.013
УДК 004.41

СИСТЕМАТИЗАЦИЯ СВЕДЕНИЙ ОБ ОШИБКАХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННОЙ КАРТЫ И ОЦЕНКА ИХ ЗНАЧИМОСТИ

А.А. Гончаров, М.А. Тарелкин, А.Л. Сердечный

В статье представляются результаты построения и анализа информационной карты, систематизирующей сведения об ошибках программного обеспечения. В качестве исходных данных была рассмотрена информация, содержащаяся в базе данных уязвимостей National Vulnerability Database. Информационная карта позволила установиться взаимосвязи между классами программного обеспечения и характерными для них типами ошибок. Систематизация сведений об ошибках программного обеспечения в виде информационной карты позволяет оценить роль соответствующего фактора при определении приоритета обработки сведений о соответствующих уязвимостях с учётом их уровня опасности. Результатом является разработка рекомендаций по приоритизации уязвимостей в целях их первоочередной обработки и применения мер защиты для минимизации ущерба от их эксплуатации. Информационная карта сведений об ошибках программного обеспечения может являться основой для наглядного отображения рисков эксплуатации уязвимостей программного обеспечения.

Ключевые слова: информационная карта, уязвимость программного обеспечения, тип ошибки программного обеспечения, CWE.

SYSTEMATIZATION OF DATA ABOUT SOFTWARE WEAKNESSES USING AN INFORMATION MAP AND ASSESSMENT OF THEIR SIGNIFICANCE

A.A. Goncharov, M.A. Tarelkin, A.L. Serdechnyy

The article presents the results of the construction and analysis of an information map systematizing information about software weaknesses. The information contained in the vulnerability database National Vulnerability Database was considered as the source data. The information map made it possible to establish the relationship between the classes of software and the types of weaknesses characteristic of them. The systematization of information about software weaknesses in the form of an information map allows us to assess the role of the relevant factor in determining the priority of processing information about the relevant vulnerabilities, taking into account their level of danger. The result is the development of recommendations on prioritizing vulnerabilities in order to process them as a priority and apply protection measures to minimize damage from their exploitation. The information map of software weaknesses can be the basis for a visual display of the risks of exploiting software vulnerabilities

Keywords: information map, software vulnerability, type of software weakness, CWE.