DOI 10.36622/VSTU.2021.24.1.001
УДК 004.415.538

ВЫЯВЛЕНИЕ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНЫХ МЕДИА НА ОСНОВЕ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ

В.А. Минаев, А.Д. Реброва, А.В. Симонов

В статье обсуждаются модели классификации текстового контента и методы его предварительной обработки с целью выявления деструктивных воздействий в социальных медиа. Показано, что основным источником деструктивного контента выступает профиль пользователей, характеризующийся набором личным данных, содержанием публикаций, параметрами сообщества, аккаунтов сети, сообщений и чатов. Говорится об актуальности автоматизированного сбора и анализа данных с помощью моделей прецедентного и дедуктивного обучения. Рассматриваются их основные разновидности и задачи, решаемые на их основе, включающие прогнозирование и типологизацию в аспекте деструктивного содержания текстов, снижение размерности признаков их описания. Исследованы и применены основные методы векторизации текстов: Bag of Words, TF_IDF, Word2vec. На практических корпусах текстов из социальной сети ВКонтакте решены задачи выявления деструктивного контента, связанного с радикальным исламом. Показано, что с помощью примененных моделей и методов все тексты, включающие деструктивный контент, классифицированы верно. Наиболее высокую точность (0,97) при решении задачи распознавания деструктивного контента дает системная интеграция алгоритма векторизации Bag of Words, метода главных компонент для снижения пространства признаков описания текстов и логистической регрессии или случайного леса как моделей обучения. Сделан вывод, что наборы данных, имеющие связь с исламским радикализмом, характеризуются достаточно четкими признаками, которые хорошо вычисляемы с помощью современных моделей, методов и алгоритмов, и могут эффективно применяться для автоматизированной классификации текстовых массивов с целью выявления их деструктивной направленности. Развитие направления, представленного в статье, связано с увеличением исследуемых корпусов документов, более детальным анализом текстов на основе сложных моделей распознавания латентной экстремистской пропаганды, в том числе – представленной в фото, аудио- и видеоформатах.

Ключевые слова: деструктивный текстовый контент, исламский радикализм, социальные медиа, распознавание негативного информационного воздействия, модель машинного обучения.

DETECTION DESTRUCTIVE CONTENT IN SOCIAL MEDIA BASED ON MACHINE LEARNING MODELS

V.A. Minaev, A.D. Rebrova, A.V. Simonov

The article discusses models of classification of text content and methods of its pre-processing in order to identify destructive influences in social media. It is shown that the main source of destructive content is the user profile, which is characterized by a set of personal data, the content of publications, community parameters, network accounts, messages and chats. Automated data collection and analysis using case-based and deductive learning models is discussed. We consider their main varieties and the tasks solved on their basis, including forecasting and typology in the aspect of the destructive content of texts, reducing the dimension of the features of their description. The main methods of text vectorization are investigated and applied: Bag of Words, TF_IDF, Word2vec. The tasks of identifying destructive content related to Islamic radicalism are solved on the practical corpus of texts from the social network VKontakte. It is shown that using the applied models and methods, all texts that include destructive content are classified correctly. The highest accuracy (0.97) in solving the problem of recognizing destructive content is provided by the system integration of the Bag of Words vectorization algorithm, the principal component method for reducing the feature space of text descriptions, and logistic regression or random forest as learning models. It is concluded that the data sets associated with Islamic radicalism are characterized by sufficiently clear features that are well calculated using modern models, methods and algorithms, and can be effectively used for automated classification of text arrays in order to identify their destructive orientation. The development of the direction presented in the article is associated with an increase in the studied corpus of documents, a more detailed analysis of texts based on complex models for recognizing latent extremist propaganda, including those presented in photo, audio and video formats.

Keywords: destructive text content, Islamic radicalism, social media, recognition of negative information impact, machine learning model.

DOI 10.36622/VSTU.2021.24.1.002
УДК 004.056.53

ОСОБЕННОСТИ РАЗМЕЩЕНИЯ БАЗ ПЕРСОНАЛЬНЫХ ДАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НАУЧНО-ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

П.Ю. Пушкин

В статье проведен анализ нормативных актов по организации обработки и защите персональных данных на предмет размещения баз данных, используемых в информационных системах российских учреждений научно-образовательной сферы. С 2015 года законодательством Российской Федерации определена необходимость размещения баз персональных данных на территории нашей страны. Однако есть случаи, когда хранение персональных данных возможно и за пределами нашей страны. В работе рассмотрены такие исключения, применимые к сфере деятельности научно-образовательных учреждений. На основе автоматизированного анализа реестра операторов персональных данных определено соотношение высших учебных заведений, представивших сведения о месте нахождения своих баз данных в соответствии с Российским законодательством. Более 24% высших учебных заведений такие сведения не предоставили, что может говорить о необходимости оказания университетскому операторскому сообществу методической помощи по вопросам порядка обработки и защиты персональных данных. В ходе проведения контроля за порядком обработки персональных данных по требованию Роскомнадзора необходимо представить, в том числе, документы, подтверждающие расположение баз персональных данных информационных систем в пределах границ Российской Федерации. В работе разработаны рекомендации по размещению и документальному оформлению местонахождения баз данных, использующихся в информационных системах научно-образовательных учреждений, при использовании собственной и предоставляемой третьими лицами ИТ-инфраструктуры.

Ключевые слова: защита персональных данных, защита баз данных, персональные данные, реестр операторов персональных данных.

FEATURES OF POSITIONING PERSONAL DATABASES OF INFORMATION SYSTEMS OF SCIENTIFIC AND EDUCATIONAL INSTITUTIONS

P.Yu. Pushkin

The article analyzes normative acts on the organization of processing and protection of personal data for the location of databases used in information systems of Russian institutions of the scientific and educational sphere. Since 2015, Russian legislation has provided for the placement of personal data bases on the territory of our state. However, there are cases when the storage of personal data is possible outside our country. The paper considers such exceptions applicable to the field of activities of scientific and educational institutions. On the basis of an automated analysis of the register of personal data operators, the ratio of higher educational institutions that provided information about the location of their databases in accordance with the legislation of the Russian Federation was determined. More than 24% of higher educational institutions did not provide such information, which may indicate the need to provide the university operator community with methodological assistance on organizing the processing and protection of personal data. In the course of state control over the organization of personal data processing, it is required to submit, among other things, documents confirming the placement of databases of personal data of information systems on the territory of the Russian Federation. Recommendations have been developed for placing and documenting the location of databases, when processing them in the information systems of research and educational institutions using their own and provided by third parties IT infrastructure.

Keywords: personal information, personal data protection, register of personal information operators.

DOI 10.36622/VSTU.2021.24.1.003
УДК 004.056

ФОРМАЛИЗАЦИЯ ПОДХОДА К ОПРЕДЕЛЕНИЮ УРОВНЯ МОТИВАЦИИ НАРУШИТЕЛЯ

О.М. Голембиовская, Е.В. Кондрашова, М.Ю. Рытов, М.М. Голембиовский

В статье рассматривается подход, связанный с определение уровня мотивации нарушителя к совершению того или иного противоправного деяния относительно ресурсов организации. Предлагаемый подход, возможно, применять службам безопасности предприятия относительно работников как при приеме на работу, так и в процессе работы с целью выявления высокого уровня мотивации к совершению противоправного деяния и выполнению различных мер по нейтрализации или минимизации данного уровня. Уровень мотивации напрямую влияет на потенциал нарушителя и на вероятность реализации им угрозы, так как не только наличие на объекте средств защиты или наличие у нарушителя современных средств атак приводит к реализации угрозы. В первую очередь к ней приводит заинтересованность в совершении данного деяния, мотивируемость и цели, которые преследует нарушитель.

Ключевые слова: модель нарушителя, мотивация, лояльность, информационная безопасность, защита информации.

FORMALIZATION OF THE DEFINITION APPROACH THE LEVEL OF MOTIVATION OF THE VIOLATOR

O.M. Golembiovskaya, E.V. Kondrashova, M.Y. Rytov, M.M. Golembiovsky

The article considers an approach related to determining the level of motivation of the violator to commit a particular illegal act with respect to the resources of the organization. The proposed approach can be applied by the security services of the enterprise in relation to employees both when hiring and in the process of work in order to identify a high level of motivation to commit an illegal act and to implement various measures to neutralize or minimize this level. The level of motivation directly affects the potential of the violator and the probability of the threat implementation, since not only the presence of protective equipment on the object or the presence of modern means of attack on the violator leads to the implementation of the threat. First of all, it leads to the interest in the commission of this act, the motivation and goals that the violator pursues.

Keywords: intruder model, motivation, loyalty, information security, information protection.

DOI 10.36622/VSTU.2021.24.1.004
УДК 004.056.53

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ КОМПЬЮТЕРНЫХ АТАК, РЕАЛИЗУЕМЫХ ГРУППИРОВКОЙ APT3 В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.Л. Сердечный, А.В. Айдаркин, М.А. Тарелкин, А.Е. Дешина

В работе представлены результаты моделирования способов реализации долговременных целенаправленных атак на корпоративные распределённые компьютерные системы со стороны одной из опасных киберпреступных группировкок – Advanced Persistent Threat 3 (APT3). Осуществлено моделирование способов, реализуемых APT3. Построение моделей осуществлялось с использованием аппарата сетей Петри на основании сведений о технических приёмах, содержащихся в базе данных MITRE ATT&CK. Разработанные модели взаимосвязаны по условиям и последствиям реализации основных технических приёмов, актуальных для корпоративных распределённых компьютерных сетей. Реализованный подход также позволяет моделировать меры защиты, регламентируемые нормативными и методическим документами, что даст возможность принятия обоснованных решений при построении системы защиты с учётом специфики защищаемого объекта.

Ключевые слова: киберпреступные группировки, APT-атаки, сети Петри, ATT&CK, APT 3, распределенные компьютерные системы.

MODELING, ANALYSIS AND COUNTERING SCENARIOS OF PREPARING COMPUTER ATTACKS REALIZED BY THE GROUP APT3 IN DISTRIBUTED COMPUTER SYSTEMS

A.L. Serdechnyy, A.V. Aydarkin, M.A. Tarelkin, A.E. Deshina

The paper presents the results of modeling methods for implementing APT-attacks on corporate distributed computer systems by one of the most dangerous cybercrime groups – Advanced Persistent Threat 3 (APT3). The methods implemented by APT3 are modeled. The models were constructed using the Petri nets apparatus based on the information about technical techniques contained in the MITRE ATT&CK database. The developed models are interrelated in terms of the conditions and consequences of the implementation of the main technical techniques relevant for corporate distributed computer networks. The implemented approach also allows to model the protection measures from regulatory and methodological documents, which will make it possible to make informed decisions when building a protection system, taking into account the specifics of the protected object.

Keywords: cybercrime groups, APT attacks, Petri nets, ATT&CK, APT 3, distributed computer systems.

DOI 10.36622/VSTU.2021.24.1.005
УДК 004.052.2:003.26

ОЦЕНКА СТОЙКОСТИ ПОТОЧНЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ, ФУНКЦИОНИРУЮЩИХ В СОСТАВЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ

Н.М. Радько, С.С. Тихонова, А.Н. Мокроусов

Целью исследования является повышение защищенности телекоммуникационных систем управления в контексте криптографической защиты с использованием математического аппарата риск-анализа для оценки стойкости поточных криптосистем. Стойкость поточной криптосистемы в работе рассмотрена как совокупность рисков разнородных компонентов поточной криптосистемы, уязвимых к деструктивному воздействию. В ходе исследования проанализированы уязвимости компонентов поточной криптосистемы, особенности среды функционирования, построены модель угроз и риск-модель атакуемой поточной криптосистемы, предложены мероприятия по снижению рисков поточных криптосистем. Полученные результаты могут быть использованы или адаптированы при необходимости повышения стойкости поточных криптосистем на этапах проектирования и модернизации, а также при необходимости восстановления эффективности функционирования после компрометации или взлома. На основе предложенной риск-модели поточной криптосистемы в дальнейшем возможна реализация программного обеспечения для оценки стойкости поточных криптосистем.

Ключевые слова: поточная криптосистема, уязвимость, угроза, риск.

EVALUATION OF PERSISTENCE OF STREAMING CRYPTOSYSTEMS OPERATING AS PART OF TELECOMMUNICATIONS MANAGEMENT NETWORK SYSTEM

N.M. Radko, S.S. Tikhonova, A.N. Mokrousov

The aim of the article consists in increasing of security level of telecommunications management network system due to cryptographic security methods. Risk analysis is used as an instrument of evaluation of persistence of streaming cryptosystems. The vulnerabilities of components and features of environment are analyzed. The threat model and the risk model of the stream cryptosystem are built. Measures of reducing the risks of stream cryptosystems are proposed. The obtained results can be used or adapted if it is necessary to increase the persistence of streaming cryptosystems during the design and modernization stages, as well as if it is necessary to restore operational efficiency after compromising or hacking. Based on the proposed risk model of a stream cryptosystem, it is further possible to implement software to assess the persistence of stream cryptosystems.

Keywords: streaming cryptosystem, vulnerability, threat, risk.

DOI 10.36622/VSTU.2021.24.1.006
УДК 004.056.53:004.75:004.735

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА КОРПОРАТИВНЫЕ РАСПРЕДЕЛЕННЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ

А.Л. Сердечный, А.А. Шевелюхин, М.А. Тарелкин, А.В. Бабурин

В настоящей статье представлены результаты моделирования способов реализации компьютерных атак на корпоративные распределенные компьютерные системы. Предложенные модели способов предназначены для формирования методического обеспечения расчета рисков и выявления оценки защищенности таких систем от актуальных сценариев реализации угроз безопасности информации, которое даёт возможность обоснованного выбора мер защиты. Построение моделей способов реализации компьютерных атак осуществлялось с использованием аппарата сетей Петри на основании сведений, содержащихся в базе данных MITRE ATT&CK. Разработанные модели взаимосвязаны по условиям и последствиям реализации основных технических приёмов, определённых в базе данных ATT&CK и актуальных для корпоративных распределённых компьютерных сетей (условия и последствия моделируются позициями сети Петри, а сами технические приёмы – переходами сети Петри). Также в статье продемонстрирована возможность наращивания модели за счёт включения в неё моделей мер защиты, используемых в нормативных и методических документах ФСТЭК России.

Ключевые слова: корпоративные распределённые компьютерные систем, способы реализации компьютерных атак, ATT&CK, сети Петри, моделирование мер защиты.

MODELING, ANALYSIS AND COUNTERING SCENARIOS OF INFORMATION SECURITY THREATS ON CORPORATE DISTRIBUTED COMPUTER SYSTEMS

A.L. Serdechnyy, A.A. Sheveliukhin, M.A. Tarelkin, A.V. Baburin

This article presents the results of modeling computer attack methods on corporate distributed computer systems. The proposed models of methods are intended for the formation of methodological support for calculating risks and identifying the assessment of the security of such systems from current scenarios of information security threats, which makes it possible to choice of informed security measures. The model development of ways to implement computer attacks was carried out using the Petri nets approach based on the information contained in the MITRE ATT&CK database. The developed model is interconnected on the conditions and consequence of the basic techniques defined in the database ATT&CK and relevant for enterprise distributed computer networks (conditions and consequence are simulated positions Petri nets themselves and techniques – transitions Petri nets). In addition, the article demonstrates the possibility of increasing the model by including models of protection measures against the considered methods of implementing computer attacks, defined in the regulatory and methodological documents of the FSTEC of Russia

Key words: corporate distributed computer systems, model of computer attacks methods, ATT&CK, Petri nets, modeling of security measures.

DOI 10.36622/VSTU.2021.24.1.007
УДК 004.056.52:004.735

РАЗРАБОТКА СРЕДСТВ МАСКИРОВАНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ ПОДВИЖНОЙ ЦИФРОВОЙ ЗАЩИЩЕННОЙ СВЯЗИ

Н.М. Радько, А.А. Караханова

Целью исследования является повышение защищенности цифровых данных, передаваемых в телекоммуникационных сетях подвижной цифровой защищенной связи от атак, нацеленных на нарушение конфиденциальности этих данных, за счет создания соответствующего методического обеспечения оценки и регулирования рисков успешности вышеупомянутых атак. В работе проводится анализ алгоритмов и методов, используемых злоумышленниками в ходе организации и проведения атак на защищаемые цифровые данные. Полученные результаты могут быть использованы как для более эффективной информационной защиты цифровых данных в телекоммуникационных сетях подвижной цифровой защищенной связи, так и как базис для дальнейших исследований.

Ключевые слова: телекоммуникационная сеть, цифровые данные, информационная безопасность.

DEVELOPMENT OF MASKING MEANS OF DIGITAL INFORMATION IN TELECOMMUNICATION NETWORKS OF MOBILE DIGITAL SECURED COMMUNICATIONS

N.M. Radko, A.A. Karakhanova

The aim of the study is to increase the security of digital data transmitted in the telecommunications system of mobile digital secure communications from attacks aimed at violating the confidentiality of these data, by creating an appropriate methodological support for assessing and regulating the risks of success of the above attacks. The paper analyzes the algorithms and methods used by cybercriminals in the course of organizing and carrying out attacks on protected digital data. The results obtained can be used both for more effective information protection of digital data in telecommunication systems of mobile digital secure communications, and as a basis for further research.

Keywords: telecommunication network, digital data, information security.

DOI 10.36622/VSTU.2021.24.1.008
УДК 004.056.53:004.735

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ КОМПЬЮТЕРНЫХ АТАК, РЕАЛИЗУЕМЫХ ГРУППИРОВКОЙ APT29 В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.Л. Сердечный, П.С. Краюшкин, М.А. Тарелкин, Ю.К. Язов

Статья посвящена моделированию компьютерных атак на распределённые корпоративные компьютерные системы, на примере действий группировки Advanced Persistent Threat 29 (APT29). В статье предлагается подход моделирования способов, реализуемых указанной группировкой, а также мер защиты от них. Подход основан на использовании аппарата сетей Петри, а также сведений о технических приёмах, предоставляемых в рамках проекта MITRE ATT&CK. Разработанные модели учитывают связи по условиям и последствиям действий, совершаемых группировкой APT29 в ходе атак на распределённые корпоративные системы. Также в статье продемонстрирована возможность наращивания модели за счёт включения в неё моделей мер защиты от рассмотренных способов реализации компьютерных атак. Предлагаемые модели могут быть дополнены за счёт моделирования новых способов реализации компьютерных атак, используемых другими кибергруппировками. Кроме того, модели могут быть расширены до моделей сети Петри-Маркова путём реализации частным методик расчёта вероятностно-временных характеристик для фрагментов предлагаемых моделей.

Ключевые слова: киберпреступные группировки, APT-атаки, сети Петри, ATT&CK, APT 29, распределенные компьютерные системы.

MODELING, ANALYSIS AND COUNTERING SCENARIOS OF PREPARING COMPUTER ATTACKS REALIZED BY THE GROUP APT29 IN DISTRIBUTED COMPUTER SYSTEMS

A.L. Serdechnyy, P.S. Krayushkin, M.A. Tarelkin, Y. K. Yazov

The article is devoted to modeling computer attacks on distributed corporate computer systems, using the example of the actions of the Advanced Persistent Threat 29 (APT29) group. The article proposes an approach to modeling the methods implemented by this grouping, as well as measures to protect against them. The approach is based on Petri nets and information about the techniques (MITRE ATT&CK project). The developed models take into account the relationship between the conditions and consequences of actions committed by the APT29 group during attacks on distributed enterprise systems. The article also demonstrates the possibility of increasing the model by including models of protection measures against the considered methods of implementing computer attacks. The proposed models can be supplemented by modeling new ways of implementing computer attacks used by other cyber groups. In addition, the models can be extended to Petri-Markov network models by implementing special methods for calculating probabilistic-time characteristics for fragments of the proposed models.

Keywords: cybercrime groups, APT attacks, Petri nets, ATT&CK, APT 29, distributed computer systems.

DOI 10.36622/VSTU.2021.24.1.009
УДК 004.056.53:004.735

РАСЧЕТ РИСКОВ И ОЦЕНКА УГРОЗ ИСПОЛЬЗОВАНИЯ СИСТЕМ ГОЛОСОВОГО УПРАВЛЕНИЯ В ДОВЕРЕННЫХ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.А. Хайдаров, А.С. Шишлов, Н.Н. Толстых

Цель исследования состоит в повышении защищенности элементов распределенной компьютерной системы автоматического распознавания голосовых команд от возможного неверного определения команды за счет создания алгоритмического обеспечения оценки и регулирования рисков неверной идентификации голосовой команды для сравнения реализации двух алгоритмов: алгоритм динамической трансформации временной шкалы и алгоритм на основе скрытых Марковских процессов.Полученные результаты могут быть использованы или адаптированы при необходимости повышения стойкости систем автоматического распознавания голосовых команд на этапах проектирования и модернизации, а также при необходимости восстановления эффективности функционирования после компрометации или взлома.

Ключевые слова: искусственный интеллект, распознавание речи, уязвимость, угроза, риск.

A.A. Khaidarov, A.S. Shishlov, N.N. Tolstykh

RISK CALCULATION AND THREAT ASSESSMENT OF THE USE OF VOICE CONTROL SYSTEMS IN TRUSTED DISTRIBUTED COMPUTER SYSTEMS

The aim of the study is to increase the security of the elements of a distributed computer system for automatic recognition of voice commands from possible incorrect identification of the command by creating algorithmic support for assessing and managing the risks of incorrect identification of the voice command to compare the implementation of two algorithms: the algorithm for dynamic transformation of the timeline and the algorithm based on hidden Markov processes.The obtained results can be used or adapted if it is necessary to increase the stability of automatic voice recognition systems at the design and modernization stages, as well as if it is necessary to restore the efficiency of functioning after a compromise or hacking.

Keywords: artificial intelligence, speech recognition, vulnerability, threat, risk.

DOI 10.36622/VSTU.2021.24.1.010
УДК 004.056.53:004.087.4

РАЗРАБОТКА МЕТОДИЧЕСКОГО АППАРАТА ВНЕДРЕНИЯ ЗАЩИТНЫХ ФУНКЦИЙ В ОТЕЧЕСТВЕННЫХ МИКРОКОНТРОЛЛЕРАХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ПОДВИЖНОЙ ЦИФРОВОЙ ЗАЩИЩЕННОЙ СВЯЗИ

А.И. Мордовин, Д.С. Хохлова

Целю исследований является повышение защищенности данных и программного кода Flash – памяти отечественных микроконтроллеров в телекоммуникационных системах (ТКС) цифровой подвижной защищенной связи от атаки программного обеспечения (несанкционированного доступе и копирование) за счет регулирования рисков успешности вышеуказанной атаки путем разработки методического аппарата защиты кода программ. В работе продемонстрирован программный метод с использованием bootloader – загрузки программы из внешней памяти. Проведен анализ спецификаций на отечественные и зарубежные микроконтроллеры. Полученные результаты работы могут послужит обеспечению безопасности отечественных микроконтроллеров и дальнейшему развитию способов противодействия угрозам. Разработанный методический аппарат защиты кода программ от несанкционированного доступа позволит вывести отечественное оборудование на должный уровень применения, что позволит провести политику импортозамещения в части защиты кода программ.

Ключевые слова: микроконтроллер, защитные функции, микросхема памяти, доступ к внешним интерфейсам.

DEVELOPMENT OF METODOLOGYCAL APPARATUS FOR IMPLEMENTATION OF PROTECTIVE FUNCTIONS IN DOMESTIC MICROCONTROLLERS IN MOBILE DIGITAL PROTECTED COMMUNICATION

A.I. Mordovin, D.S. Khokhlova

The purpose of research is to increase the security of data and Flash program code - the memory of domestic microcontrollers in the digital mobile communication system from software attacks (unauthorized access and copying) due to the management of the risks of success of the above attack by developing a methodological device for protecting program code. The work demonstrates a software method using bootloader - loading a program from external memory. Analysis of specifications for domestic and foreign microcontrollers. The results of the work can serve to ensure the safety of domestic microcontrollers and the further development of ways to counter threats. The developed methodological apparatus for protecting program code from unauthorized access will bring domestic equipment to the proper level of application, which will allow for an import substitution policy regarding program code protection.

Keywords: microcontroller, security function, memory chip, access to external interfaces.

DOI 10.36622/VSTU.2021.24.1.011
УДК 004.056.53:004.735

ОЦЕНКА РИСКОВ УСПЕШНОЙ РЕАЛИЗАЦИИ СПУФИНГ-АТАК НА ЭЛЕМЕНТЫ ГОЛОСОВОЙ АУТЕНТИФИКАЦИИ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А. А. Хайдаров, С. А. Бодячевский, Н. Н. Толстых

Цель исследования заключается в рекомендациях по улучшению мер защиты голосовых систем аутентификации от реализации спуфинг-атак. В работе рассмотрены разнообразные виды спуфинг-атак и выделены самые опасные на данный момент. Разработана методика оценки защищенности голосовых систем аутентификации, учитывающая воздействие различных видов спуфиг-атак на системы голосовой аутентификации. Проведены количественные эксперименты, показывающие преимущество разработанной методики, в сравнении с существующими аналогами. Описан комплекс программных средств оценки защищенности систем голосовой аутентификации, который позволяет автоматизировать процесс оценки при проведении технологических испытаний. Полученные результаты могут быть использованы не только для оценки защищенности систем голосовой аутентификации, но и для проведения функционального и нагрузочного тестирования. Применение предложенного комплекса и методики оценки в дальнейшем может помочь в разработке технических решений по увеличению защищенности голосовых биометрических систем от реализации спуфинг-атак.

Ключевые слова: оценка рисков, спуфинг-атаки, голосовая аутентификация.

RISK ASSESSMENT OF SUCCESSFUL IMPLEMENTATION OF SPOOFING ATTACKS ON VOICE AUTHENTICATION ELEMENTS IN DISTRIBUTED COMPUTER SYSTEMS

A.A. Khaidarov, S.A. Bodyachevskiy, N.N. Tolstykh

The purpose of the study is to provide recommendations for improving the protection of voice authentication systems against spoofing attacks. The paper considers various types of spoofing attacks and identifies the most dangerous ones at the moment. A method for assessing the security of voice authentication systems has been developed, taking into account the impact of various types of spoofing attacks on voice authentication systems. Quantitative experiments were carried out, showing the advantage of the developed method in comparison with existing analogues. A set of software tools for assessing the security of voice authentication systems is described, which allows you to automate the evaluation process during technological tests. The results obtained can be used not only to assess the security of voice authentication systems, but also to conduct functional and load testing. The use of the proposed complex and evaluation methodology in the future can help in the development of technical solutions to increase the security of voice biometric systems from spoofing attacks.

Keywords: risk assessment, spoofing attacks, voice authentication.

DOI 10.36622/VSTU.2021.24.1.012
УДК 004.942:519.876.5:004.032.26

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ СЕТЕЙ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ НА РАЗНЫХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА СИСТЕМ В УСЛОВИЯХ ОТСУТСТВИЯ СТАТИСТИКИ УЩЕРБА

С.А. Ермаков, С.Ю. Громовиков, А.А. Болгов, Е.А. Москалева

В данной статье предлагается методика количественной оценки рисков успешной реализации атак, направленных на нарушение конфиденциальности данных на этапе проектирования систем, основанная на применении нейро-нечетких сетей. Представлен программный инструментарий, для выбора оптимальной конфигурации системы, который позволяет выбирать и сравнивать различные конфигурации выбранных устройств, и как итог, выбрать наиболее оптимальную для себя конфигурацию. Получена методика количественной оценки риска на этапе начала эксплуатации систем в условиях отсутствия статистики ущерба, несмотря на качественный характер входных параметров, оцененных экспертами. Данная методика основана на многокаскадном применении логического интерфейса Мамдани. Декомпозиция оцениваемых параметров позволяет уменьшить влияние субъективных оценок экспертов на исследуемый объект. Предложенная методика реализована с помощью имитационного программного комплекса.

Ключевые слова: промышленный интернет вещей, сеть, риск, экспертные оценки, нечеткие множества, эффективность, защищенность.

ASSESSMENT AND MANAGEMENT OF RISKS OF INDUSTRIAL INTERNET OF THINGS NETWORKS AT DIFFERENT STAGES OF THE SYSTEM LIFE CYCLE IN THE ABSENCE OF DAMAGE STATISTICS

S.A. Ermakov, S.U. Gromovikov, A.A. Bolgov, E.A. Moskaleva

This article proposes a method for quantifying the risks of successful implementation of attacks aimed at violating data confidentiality at the system design stage, based on the use of neuro-fuzzy networks. The software toolkit for selecting the optimal system configuration is presented, which allows you to select and compare different configurations of selected devices, and as a result, choose the most optimal configuration for yourself. A method for quantifying the risk at the start-up stage of systems operation in the absence of damage statistics is obtained, despite the qualitative nature of the input parameters evaluated by experts. This technique is based on the multi-stage application of the Mamdani logic interface. The decomposition of the estimated parameters makes it possible to reduce the influence of subjective expert assessments on the object under study. The proposed method is implemented using a simulation software package.

Keywords: industrial Internet of Things, network, risk, expert assessments, fuzzy sets, efficiency, security.

DOI 10.36622/VSTU.2021.24.1.013
УДК 004.043

ПРИНЦИПЫ УПРАВЛЕНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИМИ СТРУКТУРАМИ ПРИ ИНФОРМАЦИОННЫХ РЕСТРИКЦИЯХ В УСЛОВИЯХ ПАНДЕМИИ

В.А. Минаев, К.М. Бондарь

В статье рассматривается применение ментальных карт для решения проблем обеспечения В статье рассматривается новый сетецентрический подход к управлению социальными и экономическими структурами в условиях пандемических ограничений, базирующийся на применении современных информационных технологий и сетевой организации информационного обмена. Рассматриваются информационно связанные структуры, состоящие из малых и средних предприятий, а также различных сообществ (молодежь, пенсионеры, профессиональные и иные организации). Обсуждается принцип самосинхронизации и вводится понятие “аттрактор” при сетецентрическом построении управления такими структурами. Обосновывается приоритет стратегии “заимствования” при применении механизмов диффузии инноваций в экономику и социальную жизнь регионов России. Предлагается полисетевая схема инновационного развития социально-экономической сферы. Она дает возможность построить инновационную инфраструктуру с применением достижений в разработке бизнес-сетей сотрудничества, а также моделей активного воздействия на общественное сознание в социальных сетях. Показана важная роль математических моделей распространения информации в социальных сетях с учетом территориальных различий для эффективного управления социально-экономическими структурами в регионах России в условиях пандемии. Найдены динамические функциональные зависимости, позволяющие отделять одни поселения от других по степени восприимчивости населения к информационному воздействию социально-экономического характера в социальных сетях, что дает возможность целенаправленно строить и реализовывать как экономические, так и социальные программы, бизнес-политику в том или ином кластере. Полученное географически компактное распределение поселений по кластерам дает возможность углубленного исследования причин региональных различий скорости распространения информации, что открывает способы оптимального информационного воздействия на региональную экономику, образовательную систему, бизнес-структуры, социальные образования (сообщества пенсионеров, молодежные структуры, клубы по интересам и т. п.) с целями их консолидации, перевода на инновационные пути развития, выработки перспективных средств и методов ведения бизнеса, стимулирования экономики в сложных условиях пандемической ситуации.

Ключевые слова: социальные и экономические структуры, сетецентрическая модель управления, пандемия, информационные технологии, самосинхронизация, аттрактор, стратегия “заимствования”, образовательный сегмент, кластер.

PRINCIPLES OF SOCIO-ECONOMIC STRUCTURES MANAGING FOR INFORMATION RESTRICTIONS IN THE PANDEMIC CONDITIONS

V.A. Minaev, K.M. Bondar

The article discusses the theoretical and applied aspects of a new network-centric approach to managing social and economic structures under pandemic restrictions. The model is based on the use of modern information technologies and the network organization of information exchange. Networks are considered as aggregations of information-related structures consisting of small and medium-sized enterprises, as well as various communities (youth, pensioners, professional and other organizations. The principle of self-synchronization in the network-centric construction of management of such structures is considered. The concept of “attractor” is introduced. The strategy of “borrowing” in the application of innovations diffusion mechanisms in the economy and social life of the Russia regions is justified. A multi-network scheme of innovative development of the socio-economic sphere is proposed, including the educational segment, among them – the development of electronic forms of education. It provides an opportunity to create an innovative infrastructure in our country using achievements in the development of business cooperation networks, as well as models of active influence on public consciousness in social networks. The article shows the important role of mathematical models of information propagation in social networks, taking into account territorial differences, for the effective management of socio-economic structures in the regions of Russia in the context of a pandemic.

Dynamic functional dependencies are found that allow separating some settlements from others according to the degree of susceptibility of the population to the information influences of a socio-economic nature in social networks, which makes it possible to purposefully create and implement both economic and social programs, business policies in a particular cluster. Received geographically compact allocation of settlements across clusters allows in-depth to explore the causes of regional differences in the speed of information propagation, which opens the ways of informational influence on the regional economy, educational system, businesses, social formation (community of pensioners, youth structures, clubs of interest, etc.) with the purpose of their consolidation, formation of promising means and methods of doing business, stimulating the economy in the difficult conditions of the pandemic situation.

Keywords: social and economic structures, network-centric management model, pandemic, information technologies, self-synchronization, attractor, “borrowing " strategy, educational segment, cluster.