DOI 10.36622/VSTU.2021.24.4.001
УДК 004.056.53

КАРТОГРАФИЧЕСКОЕ ИССЛЕДОВАНИЕ BLOCKCHAIN-ТРАНЗАКЦИЙ И СМАРТ-КОНТРАКТОВ КИБЕРПРЕСТУПНИКОВ, АТАКУЮЩИХ АВТОМАТИЗИРОВАННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ, И ОЦЕНКА УЩЕРБОВ ОТ РЕАЛИЗАЦИИ ИХ АТАК

А.Л. Сердечный, Д.А. Скогорева, Е.П. Длинный, Т.Ч. Ле, Д.В. Чьеу

Целью настоящих исследований следует считать противодействие компьютерной преступности за счёт совершенствования методов анализа их финансовых транзакций, осуществляемых в рамках операций с криптовалютами, построенными по технологии Blockchain. В рамках исследований разработана программная система сбора и картографического анализа сведений о Bitcoin-транзакциях и смарт-контрактах, а также разработана методика её применения для решения задач, связанных с противодействием компьютерной преступности. На примере анализа деятельности криптовымогателей показана возможность использования методики для оценки рисков, связанных с соответствующими угрозами. На основании полученных оценок были разработаны рекомендации по снижению рисков от угроз воздействия криптовымогателей. Полученные результаты могут быть применены для противодействия компьютерным преступлениям на корпоративные информационные системы, а также для оценки рисков реализации других угроз, связанных с группировками, использующими криптовалюты для осуществления своей преступной деятельности.

Ключевые слова: картографический метод, Blockchain, смарт-контракты, Bitcoin, криптовымогатели, риск, ущерб.

CARTOGRAPHIC STUDY OF BLOCKCHAIN TRANSACTIONS AND SMART CONTRACTS OF CYBERCRIMINALS IN THE CONTEXT OF IMPLEMENTING ATTACKS ON AUTOMATED INFORMATION SYSTEMS AND ASSESSING THE DAMAGE TO THEIR IMPLEMENTATION

A.L. Serdechnyy, D.A. Skogoreva, E.P. Dlinnyy, T.Ch. Le, D.V. Cheu

The purpose of this study should be considered to counteract computer crime by improving the methods of analyzing their financial transactions carried out as part of operations with cryptocurrencies built on Blockchain technology.As part of the research, a software system for collecting and cartographic analysis of information about Bitcoin transactions and smart contracts has been developed, and a methodology for its application has been developed to solve problems related to countering computer crime. Using the example of the analysis of the activities of crypto ransomware, the possibility of using the methodology to assess the risks associated with the corresponding threats is shown. Based on the estimates obtained, recommendations were developed to reduce the risks from the threats of the impact of ransomware. The obtained results can be applied to counteract computer crimes on corporate information systems, as well as to assess the risks of implementing other threats associated with groups using cryptocurrencies to carry out their criminal activities.

Keywords: cartographic method, Blockchain, smart contracts, bitcoin, ransomware, risk, damage.

DOI 10.36622/VSTU.2021.24.4.002
УДК 004.7

АЛГОРИТМИЧЕСКОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РИСК-АНАЛИЗА АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «УМНЫЙ ДОМ»

С.А. Ермаков, К.Н. Петрухненко, А.А. Болгов, А.Н. Бартенев

В работе проводится сравнительный анализ существующих методик оценки и регулирования рисков, а также изучается возможность их применения в условиях использования сетей устройств умного дома в контексте их использования при проведении оценки и регулирования рисков. Предлагается оригинальная методика риск-анализа в сетях устройств умного дома, повышающая степень защищенности таких систем, которая основана как на использовании наиболее подходящих процедур из рассмотренных методик, так и на использовании аппарата нечётких чисел. Произведена первоначальная классификация угроз для систем умного дома. Разработана последовательность вычислений для типовых систем и система ввода данных, позволяющая пользователю самостоятельно задавать параметры для модели сети, что обеспечивает наибольшую точность при проведении оценки и регулировании рисков. Предложенная модель реализована при помощи разработанного программного комплекса.

Ключевые слова: риск, интернет вещей, умный дом, нечёткие числа, сетевая атака, уязвимость.

ALGORITHM AND HARDWARE FOR RISK ANALYSIS OF THE SMART HOME AUTOMATED INFORMATION SYSTEM

S.A. Ermakov, K.N. Petrukhnenko, A.A. Bolgov, A.N. Bartenev

The work provides a comparative analysis of existing risk assessment and management techniques, as well as a study of their application in the context of smart home networks in the context of their use in risk assessment and management. We propose our own methodology for assessing and managing risks in networks of smart home devices by analyzing the security of such systems, which is based both on the use of the most suitable items from the methods considered, and on the use of a device of fuzzy numbers. The initial classification of threats for smart home systems has been made. A model of calculations for typical systems and a data input system have been developed, allowing the user to independently set parameters for the network model, which ensures the greatest accuracy in conducting risk assessment and management. The proposed model is implemented using the developed software complex.

Keywords: risk, Internet of things, smart home, fuzzy numbers, network attack, vulnerability.

DOI 10.36622/VSTU.2021.24.4.003
УДК 004.056.53

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ РЕАЛИЗАЦИИ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ДАННЫМ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «УМНЫЙ ДОМ»: МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

В.Е. Кунавин, С.А. Ермаков, А.А. Болгов, С.В. Лихобабин

В работе проводится разработка методического подхода и программного обеспечения оценки и регулирования рисков реализации угроз несанкционированного доступа к данным автоматизированной информационной системы «Умный дом». Предлагается оригинальный подход к анализу защищенности таких систем, основанный на применении аппарата теории рисков и нечёткой логики. Произведен анализ существующих подходов к обеспечению безопасности информационных систем. Построена методическая база оценки рисков и рекомендации по их регулированию. Предложенный методический подход реализован с помощью имитационного программного комплекса. Предложена методика регулирования рисков, основанная на анализе состояния межмашинного взаимодействия внутри сети с течением времени. Произведена оценка эффективности методического подхода к оценке и управлению рисками.

Ключевые слова: риск, интернет вещей, умный дом, нечёткая логика, сетевая атака.

ASSESSMENT AND REGULATION OF THE RISKS OF THE REALIZATION OF THREATS OF UNAUTHORIZED ACCESS TO THE DATA OF THE AUTOMATED INFORMATION SYSTEM "SMART HOME": METHODOLOGICAL BASE AND SOFTWARE

V.E. Kunavin, S.A. Ermakov, A.A. Bolgov, S.V. Likhobabin

The work contains a methodological approach and software for assessing and regulating the risks of the implementation of threats of unauthorized access to the data of the automated information system "Smart House". An original approach to the analysis of the security of such systems is proposed, based on the use of the theory of risks and fuzzy logic. The analysis of existing approaches to ensuring the security of information systems has been carried out. A methodological basis for assessing risks and recommendations for their regulation has been built. The proposed methodological approach is implemented using a simulation software package. A risk management methodology based on the analysis of the state of machine-to-machine interaction within the network over time is proposed. The effectiveness of the methodological approach to risk assessment and management was assessed.

Keywords: risk, internet of things, smart home, fuzzy logic, network attack.

DOI 10.36622/VSTU.2021.24.4.004
УДК 004.942

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОВИД-ИНФОДЕМИИ

И.В. Щетинина, Е.А. Москалева, М.Е. Волкова, В.К. Власов

Цель исследования состоит в разработке методики и поиске эффективного алгоритма Инфодемия представляет собой стремительное и неконтролируемое распространение в медиа необоснованной и ложной информации о кризисных событиях. Во время пандемии коронавируса возникла новая разновидность сетевой дезинформации, связанная с распространением различных слухов о заболевании, вакцинации и т. п., которая стремительно развиваясь, охватила все страны, став таким образом ковид-инфодемией. Инфодемия наносит большой вред работе систем здравохранения, правительств стран, существенно снижая уровень доверия к ним граждан. В статье представлена математическая модель инфодемии, основанная на данных по статистике о слухах, посвященных коронавирусной пандемии. За основу взяты эпидемические SEIR и SEIR-D модели. Результаты моделирования показали применимость предлагаемых моделей. Предлагаемые в статье модели можно использовать для прогнозирования развития и моделирования угроз ковид-инфодемии, в задачах определения ущерба, наносимого ковид-инфодемией экономике и здравохранению.

Ключевые слова: инфодемия, эпидемическая модель, информационная безопасность, коронавирусная инфодемия.

COVID-INFODEMY MATHEMATICAL MODEL

I.V. Shetinina, E.A. Moskaleva, M.E. Volkova, V.K. Vlasov

Infodemia is the rapid and uncontrolled dissemination of unreasonable and false information about crisis events in the media. During the coronavirus pandemic, a new type of online misinformation has emerged, associated with the spread of various rumors about the disease, vaccinations, etc., which is rapidly developing, spreading across all countries, thus becoming a covid infodemic. Infodemia causes great harm to the work of health care systems, governments of countries, significantly reducing the level of citizens' trust in them. The article presents a mathematical model of infodemic, based on statistics on rumors about the coronavirus pandemic. Epidemic SEIR and SEIR-D models are taken as a basis. The simulation results showed the applicability of the proposed models. The models proposed in the article can be used to predict the development and modeling of the threats of covid-infodemia, in the tasks of determining the damage caused by covid-infodemy to the economy and health care.

Keywords: infodemic, epidemic model, information security, coronavirus infodemic.

DOI 10.36622/VSTU.2021.24.4.005
УДК 004.415.25

РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО ПРОГРАММНОГО МОДУЛЯ РЕГИОНАЛЬНОГО ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЯ

А.Ю. Каушан, А.В. Поздникина, А.Г. Остапенко, А.С. Пахомова, И.А. Боков

В статье рассмотрена корреляция факторов влияния на уязвимость к деструктивному контенту в социальных сетях и параметров интернет-пользователя. В этой связи авторами предлагается методология, а также программная реализация, позволяющая определять подверженные деструктивному воздействию в сети страты региональных интернетпользователей. Практический смысл предлагаемой работы заключается в том, что благодаря данной методологии появилась возможность на основе социального опроса пользователей интернет пространства с помощью статистической вероятности оценить шанс попадания под негативное воздействие деструктивного контента. При достаточной общности предлагаемой методики акцент сделан на региональный аспект. Все это в совокупности образует полную методологию, которая может служить основой для дальнейших исследований, проводимых в данной сфере, а также использоваться для выработки рекомендации по снижению уязвимости пользователей регионального интернет-пространства от влияния деструктивного контента.

Ключевые слова: социальная сеть, деструктивный контент, безопасный интернет.

DEVELOPMENT OF AN AUTOMATED SOFTWARE MODULE FOR A REGIONAL INTERNET USER

A.Y. Kaushan, A.V. Pozdnikina, A.G. Ostapenko, A.S. Pahomova, I.A. Bokov

The paper studies the correlation of factors of influence on the vulnerability to destructive content in social networks from the parameters of the Internet user. In this regard, the authors propose a methodology, as well as a software implementation, which makes it possible to identify vulnerable strata of regional Internet users. The practical meaning of the proposed work lies in the fact that thanks to this methodology, it became possible, based on a survey of Internet users, using the statistical probability of the chance of falling under the negative impact of destructive content. With sufficient generality of the proposed methodology, the emphasis is placed on the regional aspect. All this taken together forms a complete methodology, which can serve as a basis for further research in this area, and also be used to develop recommendations for reducing the vulnerability of users of the regional Internet space from the influence of destructive content.

Keywords: social network, destructive content, safe internet.

DOI 10.36622/VSTU.2021.24.4.006
УДК 004.853

РИСК-МОНИТОРИНГ КОММЕНТАРИЕВ В АВТОМАТИЗИРОВАННЫХ СОЦИАЛЬНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

А.Г. Остапенко, А.С. Пахомова, М.В. Лопатченко, Е.Ю. Чапурин, Т.Ю. Мирошниченко

Цель исследования заключается в повышении защищенности пользователей автоматизированной социальной сети «ВКонтакте» за счет использования алгоритма проведения риск-мониторинга комментариев, оставленных на публикуемый контент деструктивной направленности, с использованием средств искусственного интеллекта. Разработан возможный алгоритм риск-мониторинга комментариев с использованием средств искусственного интеллекта, позволяющий самостоятельно определять комментарии, имеющие деструктивную направленность. Алгоритм разработан с целью повышения защищенности пользователя от влияния контента деструктивной направленности в онлайн-сообществах города Воронеж, а также для дальнейшего его внедрения в программный продукт «Netepidemic-CMSN». Для его реализации были определены наиболее подходящие методы машинного обучения алгоритма, разработана метрология комментариев в автоматизированной социальной сети, а также процесс обработки данных, благоприятный для эффективного обучения алгоритма искусственного интеллекта. Также представлено информационное и алгоритмическое обеспечение разработанного метода.

Ключевые слова: автоматизированная социальная сеть, онлайн-сообщества, риск-мониторинг, искусственный интеллект, контент.

RISK MONITORING OF COMMENTS IN AUTOMATED SOCIAL NETWORKS USING ARTIFICIAL INTELLIGENCE

A.G. Ostapenko, A.S. Pakhomova, M.V. Lopatchenko, E.Yu. Chapurin, T.Yu. Miroshnichenko

The purpose of the study is to increase the security of users of the automated social network VKontakte by using an algorithm for risk monitoring of comments left on published content of a destructive nature using artificial intelligence. A possible algorithm for risk monitoring of comments using artificial intelligence has been developed, which allows one to independently determine comments with a destructive orientation. The algorithm was developed with the aim of increasing the user's protection against the influence of destructive content in the online communities of the city of Voronezh, as well as for its further implementation in the software product "Netepidemic-CMSN". For its implementation, the most suitable methods of machine learning of the algorithm were determined, metrology of comments in an automated social network was developed, as well as a data processing process favorable for effective training of an artificial intelligence algorithm. The informational and algorithmic support of the developed method is also presented.

Keywords: automated social network, online communities, risk monitoring, artificial intelligence, content.

DOI 10.36622/VSTU.2021.24.4.007
УДК 004.942

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КОМПЛЕКСА МОДЕЛИРОВАНИЯ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ С УЧЕТОМ ДОЗИРОВКИ ВИРУСОВ: МОДЕЛЬ «БАХЧИСАРАЙСКИЙ ФОНТАН»

А.Г. Остапенко, Е.А. Шварцкопф, А.А. Остапенко, В.В. Сафронова, К.В. Сибирко, Е.А. Болгова

В работе предлагается принципиально новый подход к описанию сетевых эпидемических процессов. Авторы предлагают при моделировании процесса диффузии вредоноса учитывать его дозировку в элементах исследуемой сети. В этой связи вводятся соответствующие параметры (скорость размножения вируса, пороги концентрации вируса в узлах сети по состояниям распространения вредоноса и утраты работоспособности, пропорция дозировки вируса в сетевых трафиках), которые через заданные матрицы ресурсов взвешенной сети позволяют моделировать процесс распространения инфекции по сетевой инциденции (вплоть до программной реализации). Наряду с вышеизложенным рассматриваются приемы регулирования эпидемического процесса в предлагаемом авторами прочтении.

Ключевые слова: сеть, вирус, эпидпроцесс, ресурс, потенциал, вершина и дуга сети.

MATHEMATICAL SUPPORT OF THE COMPLEX OF MODELING OF EPIDEMIC PROCESSES TAKING INTO ACCOUNT THE DOSAGE OF VIRUSES: THE MODEL «BAKHCHISARAI FOUNTAIN»

A.G. Ostapenko, E.A. Shvartskopf, A.A. Ostapenko, V.V. Safronova, K.V. Sibirko, E.A. Bolgova

The paper proposes a fundamentally new approach to the description of network epidemic processes. The authors suggest that when modeling the process of diffusion of destructive content, its dosage in the elements of the network under study should be taken into account. In this regard, the corresponding parameters are introduced (the rate of virus reproduction, the thresholds of virus concentration in the network nodes according to the states of spread of the pest and loss of operability, the proportion of the dosage of the virus in network traffic), which, through the given matrices of weighted network resources, allow you to simulate the process of infection spread by a network incident (up to software implementation). Along with the above, the methods of regulating the epidemic process are considered in the article proposed by the authors.

Keywords: network, virus, epidemiological process, resource, potential, vertex and arc of the network.

DOI 10.36622/VSTU.2021.24.4.008
УДК 004.056.55/003.26

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ АКТИВОВ

П.Ю. Филяк, С.В. Королев, Н.В. Тебеньков

Рассматривается подход к обеспечению информационной безопасности организации с позиций системного и процессного подходов, отраженных в серии государственных стандартов, посвященных менеджменту (управлению) в сфере информационной безопасности, в основе которого находится политика информационной безопасности и, соответственно, политика доступа к информации, реализация которой начинается прежде всего с оценки информационных активов (Asset), информационных ресурсов (Assets), а затем и управления ими (Asset Management) с позиций информационной безопасности. Оценка информационных активов начинается прежде всего с их инвентаризации, для которой необходимы программно-аппаратные средства (инструментальные средства), адекватно и эффективно выполняющие указанную функцию. К таковым инструментам можно, в частности, отнести Total Network Inventory 5 (TNI) - быстрая инвентаризация сетевых компьютеров, оборудования, программного обеспечения и комплексный программный продукт Algorius Net Viewer - для мониторинга и инвентаризации, визуализации, администрирования, компьютерной сети любого уровня.

Ключевые слова: информация, информационная безопасность, политика безопасности, политики доступа, инвентаризация, информационный актив, информационные ресурсы, интерфейс, протокол, IP – маршрутизация, трассировка маршрута, сканирование портов, опрос устройств.

ENSURING THE INFORMATION SECURITY WITH THE HELP OF TOOLS FOR THE INVENTORY OF INFORMATION ASSETS

P.Yu. Filyak, S.V. Korolev, N.V. Tebenkov

The approach to ensuring the information security of an organization is considered from the position of systems′s and process approaches reflected in a series of management information security standards, for the policy of information security and, accordingly, the policy of access to information, the implementation of which begins primarily with the assessment of information assets (Asset), information resources (Assets), and then their management (Asset Management) from the standpoint of information security. Evaluation of information assets begins primarily with their inventory, which requires software and hardware (tools) that adequately and effectively perform this function. These tools include, in particular, Total Network Inventory 5 (TNI) - a quick inventory of network computers, equipment, software and the Algorithius Net Viewer - a comprehensive software product for visualization, administration, monitoring and inventory of a computer network of any level.

Keywords: information, information security, security policy, access policies, inventory, information asset, information resources, interface, protocol, IP routing, route tracing, port scanning, device polling.

DOI 10.36622/VSTU.2021.24.4.009
УДК 004.056.55/003.26

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ФОРЕНЗИКИ

П.Ю. Филяк, С.В. Королев, Н.В. Тебеньков

Представлен подход к обеспечению информационной безопасности [1] с помощью применения инструментальных средств прикладной науки о расследовании и раскрытии преступлений, связанных с компьютерной безопасностью, известной под названием форензика. Рассматриваются кратко терминология, теоретические основы и подходы данной науки, а также представлен набор конкретных инструментов для реализации форензики в рамках программно-аппаратных комплексов, которые можно применять на практике в целях обеспечения информационной безопасности коммерческих и не коммерческих организаций, а также иных субъектов экономической деятельности. Представлены три программных продукта: OSForensics - комплект утилит для проведения компьютерной экспертизы, выполняющий поиск и анализ различных данных в системе, восстанавливающий данные, предоставляющий возможность просмотра следов активности пользователя; Belkasoft Evidence Center - инструмент для комплексной цифровой криминалистической экспертизы и расследования корпоративных инцидентов и Passware Kit Forensic – инструмент для поиска всех зашифрованных файлов на носителях информации.

Ключевые слова: информация, информационная безопасность, политика безопасности, политики доступа, интерфейс, идентификация, аутентификация, форензика, драйвер, утилита, дамп, анализ, пароли, стойкость паролей, событие информационной безопасности, инцидент информационной безопасности, handshake.

ENSURING THE INFORMATION SECURITY WITH THE USE OF TOOLS OF FORENSICS

P.Yu. Filyak, S.V. Korolev, N.V. Tebenkov

The paper presents an approach to ensuring information security through the use of tools of the applied science of investigation and disclosure of crimes related to computer security, known as forensics. The terminology, theoretical foundations and approaches of this science are briefly considered, as well as a set of specific tools for the implementation of forensis within the framework of software and hardware complexes that can be applied in practice in order to ensure information security of commercial and non-commercial organizations, as well as other subjects of economic activity. Three software products are presented: OSForensics - a set of utilities for conducting computer expertise, performing search and analysis of various data in the system, restoring data, providing the ability to view traces of user activity; Belkasoft Evidence Center - a tool for complex digital forensic examination and investigation of corporate incidents and Passware Kit Forensic -a tool for searching all encrypted files on data carriers.

Keywords: information, information security, security policy, access policies, interface, identification, authentication, forensics, driver, utility, dump, analysis, passwords, password strength, information security event, information security incident, handshake.

DOI 10.36622/VSTU.2021.24.4.010
УДК 004.056.53

АНАЛИЗ ДОВЕРИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИОННОГО РЕСУРСА АВТОМОБИЛЯ НА ОСНОВЕ НАВИГАЦИОННОГО КЛЮЧА

Т.З. Аралбаев, Р.Р. Галимов, А.И. Сарайкин

В статье определена актуальность задачи обеспечения информационной безопасности информационного ресурса (ИР) автомобильных транспортных средств (АТС), обусловленная увеличением степени использования информационных технологий в современных транспортных средствах и наличием уязвимостей в штатных средствах защиты. Проведен обзор литературы и выявлены недостатки существующих решений систем защиты доступа (СЗД) к ИР АТС. Определена перспективность подхода к защите ИР АТС, учитывающего взаимное расположение субъекта и объекта доступа. Предложена формализованная процедура оценки доверия к многоуровневой системе защиты доступа к ИР АТС на основе навигационного ключа, учитывающая характеристики и условия эксплуатации информационной системы, требования защиты, текущую конфигурацию мер и средств защиты. Представлены алгоритмическая модель и метод оценки доверия к системе защиты на основе системы признаков и кодов защиты. Приведены расчеты оценки доверия к системе защиты ИР автомобиля.

Ключевые слова: система разграничения доступа, информационный ресурс, автомобильное транспортное средство, навигационный ключ, система признаков, код защиты.

ANALYSIS OF TRUST IN THE PROTECTION SYSTEM OF THE INFORMATION RESOURCE OF THE VEHICLE BASED ON THE NAVIGATION KEY

T.Z. Aralbaev, R.R.Galimov, A.I. Saraikin

The article proposes a method for assessing the quality of an access protection system (APS) to information resources (IR) of a motor vehicle (MV) using a navigation key. The urgency of the tasks of ensuring the information security of IR MV is determined, due to the increase in the degree of use of information technologies in modern vehicles and the presence of vulnerabilities in the standard means of protection. The conducted literature review revealed the shortcomings of existing APS solutions to information resources of motor vehicle. The prospect of an approach to the protection of IR MV, taking into account the mutual location of the subject and the object of access, has been revealed. A model is proposed for assessing confidence in a multi-level security system for access to the IR of a motor vehicle based on a navigation key, which takes into account the characteristics and operating conditions of the MV information system, security requirements and the current configuration of security measures and means. An algorithmic model and a method for assessing the effectiveness of access protection based on a system of signs and protection codes are presented. Calculations of the quality assessment of the access protection system to IR are presented.

Keywords: access control system, information resource, automobile vehicle, navigation key, system of signs, security code.

DOI 10.36622/VSTU.2021.24.4.011
УДК 004.771

АНАЛИЗ СОВРЕМЕННЫХ ТОЧЕК ДОСТУПА БЕСПРОВОДНЫХ КАНАЛОВ ПРЕДПРИЯТИЯ

Ю.Ю. Громов, П.И. Карасев, В.В. Кулешов

В статье дается характеристика беспроводных сетей, имеющих значение для автоматизации производства, и условия для их применения. Рассмотрено применение проводной сети Ethernet, поскольку беспроводная сеть можно с легкостью в нее интегрироваться. Проведен анализ таких распространенных в автоматизации предприятий типов стандартов связи, как ZigBee и Wi-Fi. Уделено внимание проблеме взаимодействия узлов в проводных и беспроводных сетях и возможности ее решения с использованием технологии коллективного доступа с опознаванием несущей и обнаружением конфликтов. Определено, что точки доступа являются устройствами, обладающими операционными системами, в которых содержится большое количество ошибок, чем могут воспользоваться злоумышленники. Рассмотрены основные причины взлома на примере Wi-Fi и охарактеризованы методы взлома беспроводной точки доступа. Указаны способы, которые могут применяться для защиты беспроводной точки доступа. Также проведен анализ технологий, которые могут использоваться для того, чтобы защитить корпоративные сети.

Ключевые слова: беспроводные каналы, точки доступа, хендшейк; метод с использованием фишинговой точки доступа; метод подбора WPS кода, способы защиты беспроводной точки доступа.

ANALYSIS OF MODERN ACCESS POINTS FOR ENTERPRISE WIRELESS CHANNELS

Yu.Yu. Gromov, P.I. Karasev, V.V. Kuleshov

The article describes the characteristics of wireless networks that are important for the automation of production, and the conditions for their use. The application of a wired Ethernet network is considered, since a wireless network can be easily integrated into it. The analysis of such types of communication standards common in enterprise automation as ZigBee and Wi-Fi is carried out. Attention is paid to the problem of interaction of nodes in wired and wireless networks and the possibility of solving it using the technology of collective access with carrier identification and conflict detection. It is determined that access points are devices with operating systems that contain a large number of errors, which can be used by attackers. The main reasons for hacking on the example of Wi-Fi are considered and methods of hacking a wireless access point are described. The methods that can be used to protect the wireless access point are indicated, you can use the following methods. The analysis of technologies that can be used to protect corporate networks is also carried out.

Keywords: wireless channels, access points, types of communication standards, handshake interception method and its decryption; method using a phishing access point; WPS code selection method, methods of protecting a wireless access point.

DOI 10.36622/VSTU.2021.24.4.012
УДК 004.056.5

К ВОПРОСУ О СОЗДАНИИ ПЛАТФОРМЫ КАРТОГРАФИРОВАНИЯ РИСКОВ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА

А.Л. Сердечный, А.А. Гончаров, М.А. Булычев, А.В. Коноплин, О.С. Газизянов, Р.О. Дыкин, Д.С. Нестеров, Д.А. Нархов

Статья посвящена перспективам создания платформы картографирования рисков защищаемого киберпространства, потребность в которой обусловлена нарастанием неопределённости в отношении процессов, протекающих в киберпространстве. Наглядное представление таких процессов позволяет своевременно выявлять и провести исследование опасных тенденций для безопасности личности, общества и государства. В данной работе формулируются цели, задачи и функциональные требования к платформе картографирования рисков. Представленные результаты основаны на практическом опыте разработки и применения методологии картографирования защищаемого киберпространства, который был получен в ходе разработки системы картографирования рисков защищаемого киберпространства (прототип разрабатываемой платформы). Целью создания платформы является объединение усилий множества исследователей киберпространства благодаря обеспечению совместной работы по его представлению в виде системы взаимосвязанных информационных карт. Вниманию научной общественности предлагается облик платформы картографирования рисков защищаемого киберпространства и возможные решения, которые могут быть использованы для её воплощения в виде готового продукта.

Ключевые слова: киберпространство, картографирование защищаемого киберпространства, платформа картографирования рисков.

TOWARDS THE PROTECTED CYBERSPACE RISK MAPPING PLATFORM

A.L. Serdechnyy, A.A. Goncharov, M.A. Bulychev., A.V. Konoplin, O.S. Gazizyanov, R.O. Dykin, D.S. Nesterov, D.A. Narkhov

The article deals with the prospects of creating the platform for risk mapping of protected cyberspace, the need for which is due to increasing uncertainty about the processes occurring in cyberspace. A visual representation of such processes allows timely identification and investigation of dangerous trends for the security of individuals, society and the state. This paper formulates the goals, objectives and functional requirements for a risk mapping platform. The results presented are based on practical experience in the development and application of a protected cyberspace mapping methodology, which was obtained during the development of a protected cyberspace risk mapping system (prototype of the platform). The purpose of developing the platform is to bring together multiple researchers of cyberspace by enabling them to work together to represent it as a system of interconnected information maps. The scientific community is offered the appearance of the platform for risk mapping of protected cyberspace and possible solutions, which can be used for its implementation in the form of a finished product.

Keywords: cyberspace, protected cyberspace mapping, risk mapping platform.

DOI 10.36622/VSTU.2021.24.4.013
УДК 004.056

АНАЛИЗ РИСКОВ ПРИ ПОМОЩИ ИНФОРМАЦИОННОЙ КАРТЫ МУЗЫКАЛЬНЫХ ПРЕДПОЧТЕНИЙ

А.Л. Сердечный, Д.Г. Коденцева, А.А. Петелин, А.А. Лемешко, В.Е. Руженко

Роль количественной оценки рисков является ключевой в обоснованном принятии решений в отношении разработки мер защиты. Однако одного лишь интегрального значения, которое характеризует уровень опасности тех или иных видов угроз, недостаточно для полного понимания процессов, связанных с негативными воздействиями на защищаемые объекты. Отображение значений риска с помощью информационной карты позволяет не только оценить, но и «увидеть» уровень опасности с учётом особенностей «ландшафта» защищаемой системы. В настоящей работе демонстрируется реализация данной идеи на примере анализа риска вовлечения пользователей социальных сетей в группы единой тематики. Для расчёта риска используются сведения о музыкальных исполнителях, которых слушают пользователи социальной платформы ВКонтакте, состоящие в группах единой тематики. Для наглядного представления значений риска вовлечения пользователя в группу единой тематики в отношении каждого музыкального исполнителя проводится расчёт частных показателей риска, которые отображаются на информационной карте музыкальных предпочтений. Для её построения использованы данные рекомендательной системы музыкального сервиса Яндекс.Музыка. Также в статье продемонстрирована возможность использования информационных карт музыкальных предпочтений для составления и анализа профилей пользователей социальных платформ.

Ключевые слова: информационная карта музыкальных предпочтений, информационная безопасность, картографирование рисков, профиль пользователя, киберпространство.

RISK ANALYSIS BY MEANS OF A MUSICAL PREFERENCE INFORMATION MAP

A.L. Serdechnyy, N.G. Kodentseva, A.A. Petelin, A.A. Lemeshko, V.E. Ruzhenko

The role of quantitative risk assessment is key in informed decision-making regarding the development of protective measures. However, the integral value alone, which characterizes the danger level of any type threats, is not enough to fully understand the processes associated with negative impacts on protected objects. Imaging risk values using an information map allows not only to assess, but also to "see" the danger level, taking into account the features of the protected system landscape. This paper demonstrates the implementation of this idea by analyzing the risk of involving social network users in groups of the single theme. To calculate the risk, information is used about musical artists who are listened to by users of the VK social platform who are in groups of the single theme. In order to visually represent the values of the risk of involving the user in a group of the single theme, for each musical artist, the calculation of private risk indicators is carried out, which are displayed on the music map. To build it, data from the recommendation system of the Yandex.Music music service were used. The article also demonstrates the possibility of using a music map for compiling and analyzing users profiles of social platforms. Keywords: music map, information map, information security, risk mapping, user profile, cyberspace.