DOI 10.36622/VSTU.2023.26.2.001
УДК 004.056

БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ: ОСНОВНЫЕ РЕШЕНИЯ

В.А. Минаев, **Б.А. Швырев**, **Т.Р. Ромашкин**

Одной из основных проблем при обеспечении безопасности Интернета вещей (IoT) является, с одной стороны, огромное количество устройств, масштабирующее угрозы и риски безопасности их использования, а с другой – слабая разработанность или даже отсутствие стандартизированных протоколов безопасности. Нередко устройства IoT имеют ограниченную вычислительную мощность и память в угоду цене и коммерческой выгоде, что затрудняет реализацию надежных мер безопасности. Расширение IoT достигло критической инфраструктуры - системы здравоохранения, транспорта и других особо важных отраслей. Поскольку современные устройства IoT имеют доступ к персональной и конфиденциальной информации, нарушения их информационной безопасности могут иметь весьма серьезные последствия, поэтому крайне важно обосновать и реализовать надежные меры безопасности для их защиты от компьютерных атак. Проводится сравнительный анализ основных сетевые протоколов IoT. Выделяются наиболее вероятные компьютерные атаки на устройства IoT: нарушение безопасности сети, нарушение безопасности устройства, физический доступ к устройству, сбои в работе устройства, технологии социальной инженерии. Рассматриваются следующие меры для обеспечения безопасности устройств IoT: совершенствование нормативно-правовой базы; обучение и повышение квалификации сотрудников; развитие взаимодействия с производителями IoT; улучшение мониторинга IoT-устройств; улучшение методов анализа данных, связанных с функционированием IoT. Для реализации предложенных мер приводятся программные и аппаратные решения задач безопасности IoT-устройств.

Ключевые слова: Интернет вещей, угрозы информационной безопасности, протокол безопасности.

INTERNET OF THINGS SECURITY: KEY SOLUTIONS

Minaev V.A., **Shvyrev B.A.**, **Romashkin T.R.**

One of the main problems in ensuring the security of the Internet of Things (IoT) is, on the one hand, a huge number of devices that scale the threats and security risks of their use, and on the other hand, weak development or even lack of standardized security protocols. Often, IoT devices have limited computing power and memory for the sake of price and commercial benefits, which makes it difficult to implement reliable security measures. The expansion of IoT has reached critical infrastructure - healthcare, transport and other particularly important areas. Since modern IoT devices have access to personal and confidential information, violations of their information security can have very serious consequences, therefore it is extremely important to justify and implement reliable security measures to protect them from computer attacks. A comparative analysis of the main IoT network protocols is carried out. The most likely computer attacks on IoT devices are highlighted: network security violation, device security violation, physical access to the device, device malfunctions, social engineering technologies. The following measures to ensure the security of IoT devices are considered: improvement of the regulatory and legal framework; training and professional development of employees; development of interaction with IoT manufacturers; improvement of monitoring of IoT devices; improvement of data analysis methods related to the functioning of IoT. To implement the proposed measures, software and hardware solutions to the security problems of IoT devices are provided.

Keywords: Internet of Things, information security threats, security protocol.

DOI 10.36622/VSTU.2023.26.2.002
УДК 004.056

МЕТОДИЧЕСКИЕ ОСНОВЫ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫПОЛНЕНИИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ СТУДЕНТАМИ СПЕЦИАЛИТЕТА В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Г. Остапенко, А.С. Пахомова, Д.А. Нархов, А.А. Остапенко, А.И. Шеншин

В статье рассматриваются научно-методические основы реализации научно-исследовательской работы студентами специальностей в сфере обеспечения информационной безопасности. В этой связи предлагаются шаблоны формулировки противоречий и актуальности проводимого исследования. Представлены научно-обоснованные методики целеполагания, включая постановку объекта и предмета исследования, цели и задач исследования в области обеспечения информационной безопасности. К тому же предлагаются рекомендации по решению постановленных задач в условиях современного информационного противоборства государств и транснациональных корпораций. Научно-методические рекомендации, предлагаемые в статье, обильно проиллюстрированы в виде соответствующих таблиц и рисунков, позволяющих исследователю наглядно по аналогии с упомянутым иллюстративным материалом осуществлять целеполагания для своей тематике. Рассматриваются также перспективы совершенствования результатов настоящей работы в части выявления угроз, проведения риск-анализа и управления информационными рисками в ходе реализации научно-исследовательской работы студентов.

Ключевые слова: исследование, риск, безопасность, цель, задачи, объект и предмет исследования.

METHODOLOGICAL FOUNDATIONS OF PROJECT ACTIVITY WHEN PERFORMING RESEARCH WORK BY STUDENTS OF THE SPECIALTY IN THE FIELD OF INFORMATION SECURITY

A.G. Ostapenko, A.S. Pakhomova, D.A. Narkhov, A.A. Ostapenko, A.I. Shenshin

The article discusses the scientific and methodological foundations of the implementation of research work by students of specialties in the field of information security. In this regard, templates for the formulation of contradictions and the relevance of the study are proposed. The article presents scientifically-based methods of goal-setting, including the formulation of the object and subject of research, goals and objectives of research in the field of information security. In addition, recommendations are proposed for solving the tasks set in the conditions of modern information warfare between states and transnational corporations. The scientific and methodological recommendations proposed in the article are abundantly illustrated in the form of appropriate tables and figures, allowing the researcher to visually, by analogy with the above-mentioned illustrative material, carry out goal-setting for his subject. The prospects of improving the results of this work in terms of identifying threats, conducting risk analysis and managing information risks during the implementation of students' research work are also considered.

Keywords: research, risk, safety, purpose, objectives, object and subject of research

DOI 10.36622/VSTU.2023.26.2.003
УДК 004.056.47

СОЗДАНИЕ КИБЕРПОЛИГОНА: БЛОК НАВИГАЦИИ ПО СРЕДСТВАМ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

А.Л. Сердечный, А.А. Карданов, А.Т. Труфанов

В статье представлены результаты разработки блока навигации по технологиям средствам тестирования на проникновение, выполненной в рамках создания киберполигона. Блок базируется на программной реализации интерактивной информационной карты «Средства тестирования на проникновения». Информационная карта объединяет сведения о более чем 6 тыс. средств тестирования на проникновение, содержащихся в 46 различных источниках (специализированных операционных системах, таких как Kali Linux и BlackArch, научных и аналитических статьях о средствах оценки защищённости информационных систем активными методами, telegram-каналах и других информационных ресурсах). В основе информационной карты лежит граф связей между средствами тестирования на проникновение и их типами. Навигационный блок даёт возможность ознакомиться с широким составом средств, используемых для оценки защищённости информационных систем. Систематизация сведений в виде информационной карты позволяет показать сходство и различия между разными классами средств тестирования на проникновение и их отдельными представителями с учётом существования множества различных вариантов наименований, встречающихся в экспертной и научной среде. Блок навигации построен с использованием web-технологий и доступен в тестовом режиме на портале CyberMaps.ru.

Ключевые слова: киберполигон, информационная карта, информационное картографирование, тестирование на проникновение, pentest.

CREATING A CYBERPOLYGON: PENETRATION TESTING TOOLS NAVIGATION BLOCK

A.L. Serdechnyi, A.T. Trufanov, A.A. Kardanov

The article presents the results of developing a navigation block for penetration testing technologies as part of creating a cyber polygon. The block is based on software that implements an interactive information card called "Penetration Testing Tools". This information card combines information from over 6,000 penetration testing tools contained in 46 different sources, including specialized operating systems like Kali Linux and BlackArch, scientific and analytical articles on information system security assessment tools, and various other informational resources such as Telegram channels. The information map is designed based on the graph with relationships between the different types of penetration testing tools. The navigation block provides an opportunity to familiarize oneself with a wide range of tools used to assess the security of information systems. The systematization of information in the form of an information map allows readers to understand the similarities and differences between different classes of penetration testing tools and their individual representatives, considering the existence of many different names that are used in expert and scientific environments.

Keywords: cyber polygon, information map, information mapping, penetration testing, pentest.

DOI 10.36622/VSTU.2023.26.2.004
УДК 004.8

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ НАРУШЕНИЯ КРИПТОСТОЙКОСТИ КАНАЛА СВЯЗИ БЕСПРОВОДНЫХ СЕТЕЙ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ VPN

Н.М. Радько, Ю.С. Хирьянова, А.Н. Мокроусов, Е.А. Москалева

В работе представлены методические и алгоритмические способы оценки и регулирования рисков нарушения криптоустойчивости канала беспроводной связи. Особенностью рассматриваемой среды является повсеместное применение услуг VPN – протоколов, оборудования, алгоритмов шифрования. Криптостойкость канала связи беспроводных сетей с применением технологий VPN в работе рассмотрена как способность данного канала связи сохранять конфиденциальность передаваемых данных при наличии потенциальных угроз и атак со стороны злоумышленников, использующих различные методы взлома и шифрования. В научной публикации проведен анализ криптографических особенностей, функционала VPN-сервисов. На основе проведенного исследования построена математическая модель стойкости и безопасности вышеописанной технологии, предложена риск-модель атакуемого канала связи, который содержит в себе компоненты VPN. Помимо этого, выработана классификация атак на канал связи, построена риск-модель технологии VPN. Полученные в ходе исследования результаты могут быть использованы для повышения криптостойкости канала связи беспроводных сетей на этапах проектирования, а также как базис для дальнейших исследований специалистов в области информационной безопасности.

Ключевые слова: VPN, канал связи, уязвимость, риск, угроза.

RISK ASSESSMENT AND MANAGEMENT COMMUNICATION CHANNEL BREACH WIRELESS NETWORKS USING VPN TECHNOLOGIES

N.M. Radko, Yu.S. Khiryanova, A.N. Mokrousov, E.A. Moskaleva

The paper presents methodological and algorithmic methods for assessing and regulating the risks of violating the cryptographic stability of a wireless communication channel. A feature of the considered environment is the widespread use of VPN protocol services, equipment, encryption algorithms. The cryptographic strength of the communication channel of wireless networks using VPN technologies is considered in the work as the ability of this communication channel to maintain the confidentiality of transmitted data in the presence of potential threats and attacks from intruders using various methods of hacking and encryption. The scientific publication analyzes the cryptographic features and functionality of VPN services. Based on the conducted research, a mathematical model of the durability and security of the above-described technology is constructed, a risk model of the attacked communication channel is proposed, which contains VPN components. In addition, a classification of attacks on the communication channel has been developed, a risk model of VPN technology has been built.

The results obtained in the course of the study can be used to increase the cryptographic strength of the communication channel of wireless networks at the design stages, as well as basis for further research by specialists in the field of information security.

Keywords: VPN, communication channel, vulnerability, risk, threat.

DOI 10.36622/VSTU.2023.26.2.005
УДК 004.056

СОВЕРШЕНСТВОВАНИЕ ОРГАНИЗАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ: ФОРМИРОВАНИЕ РИСК-ЛАНДШАФТА СЕТЕВЫХ АТАК

Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.Ю. Пекло

В работе рассматриваются особенности формирования риск-ландшафта как основа совершенствования организационно-правового обеспечения безопасности корпоративных сетей. В этой связи осуществлено соответствующее целеполагание и намечены основные направления исследования. Применительно к риск-анализу реализована матричная формализация отношений векторов атак и используемых ими уязвимостей для заданного вида сетевого воздействия на защищаемый объект. В результате предлагается риск-ландшафт, позволяющий выявить наиболее опасные сочетания вектор-уязвимость, для противодействия которым необходимо формировать соответствующее организационно-правовое обеспечение в виде частных политик безопасности, регламентов и инструкции по защите информации корпоративной сети от сетевых атак. Предложены аналитические выражения для оценки риска успешной реализации векторов атак через сетевые уязвимости.

Ключевые слова: корпоративная сеть, вектор атак, уязвимость, политика, регламент, инструкция.

IMPROVING THE ORGANIZATIONAL AND LEGAL SUPPORT OF THE INFORMATION SECURITY OF THE ENTERPRISE: FORMING THE RISK LANDSCAPE OF NETWORK ATTACKS

G.A. Ostapenko, D.V. Shcherbakova, T.Yu. Miroshnichenko, A.A. Ostapenko, A.Yu. Peklo

The paper discusses the features of risk landscape formation as a basis for improving the organizational and legal security of corporate networks. In this regard, the appropriate goal-setting has been carried out and the main directions of research have been outlined. With regard to risk analysis, a matrix formalization of the ratios of attack vectors and the vulnerabilities used by them for a given type of network impact on the protected object is implemented. As a result, a risk landscape is proposed that makes it possible to identify the most dangerous vector-vulnerability combinations, to counter which it is necessary to form appropriate organizational and legal support in the form of private security policies, regulations and instructions for protecting corporate network information from network attacks. Analytical expressions are proposed to assess the risk of successful implementation of attack vectors through network vulnerabilities.

Keywords: corporate network, attack vector, vulnerability, policy, regulation, instruction.

DOI 10.36622/VSTU.2023.26.2.006
УДК 004.8

СОЗДАНИЕ КИБЕРПОЛИГОНА: БЛОК НАВИГАЦИИ ПО ТЕХНОЛОГИЯМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ

А.Л. Сердечный, А.Т. Труфанов, А.А. Карданов

В статье представлены результаты разработки блока навигации по технологиям искусственного интеллекта и машинного обучения, выполненной в рамках создания киберполигона. Блок базируется на программной реализации интерактивной информационной карты «Технологии искусственного интеллекта и машинного обучения». Информационная карта систематизирует сведения о задачах, методах и моделях, машинного обучения, а также наборах данных и научных публикациях, которые размещаются на информационном ресурсе Papers With Code.

Информационная карта раскрывает сложную структуру взаимосвязей между более чем 3 тыс. задач машинного обучения, 34 тыс. научных публикаций, посвящённых их решению, а также 7 тыс. наборов данных, 2 тыс. методов и алгоритмов машинного обучения, 8 тыс. моделей, упоминаемых в таких статьях. В ходе исследования информационной карты могут быть получены знаниям о современном состоянии развития технологий искусственного интеллекта, что способствует более глубокому пониманию основных тенденций в данной области, а также повышает эффективность поиска по рассматриваемой теме.

Также важным практическим значением разработанной информационной карты является возможность использования её для совместной работы по темам в области искусственного интеллекта. В качестве примера построен слой, на котором показаны области размещения и взаимосвязи между задачами, моделями и наборами данных, используемых при обеспечении информационной безопасности и защите информации.

Блок навигации построен с использованием web-технологий и доступен в тестовом режиме на портале CyberMaps.ru.

Ключевые слова: киберполигон, информационная карта, информационное картографирование, искусственный интеллект, машинное обучение.

CREATING A CYBERPOLYGON: A NAVIGATION BLOCK ON TECHNOLOGIES OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

A.L. Serdechnyi, A.T. Trufanov, A.A. Kardanov

The article presents the results of the development of the navigation block on artificial intelligence and machine learning technologies, carried out as part of the creation of a cyber polygon. The block is based on the software implementation of the interactive information map "Artificial Intelligence and Machine Learning Technologies". The information map systematizes information about tasks, methods and models, machine learning, as well as data sets and scientific publications, which are placed on the information resource Papers With Code.

The information map reveals the complex structure of relationships between more than 3,000 machine learning problems, 34,000 scientific publications devoted to their solution, as well as 7,000 datasets, 2,000 machine learning methods and algorithms, and 8,000 models mentioned in such articles. During research of an information map it is possible to receive knowledge of a current condition of development of technologies of an artificial intellect that promotes deeper understanding of the basic tendencies in the given area, and also raises efficiency of search on the considered subject.

Also an important practical value of the developed information map is the possibility of its use for crowdsourcing work in the field of artificial intelligence. As an example the layer is built, which shows the areas of placement and relationships between tasks, models and data sets used in information security and information protection.

Navigation block is built using web-technology and is available in test mode on the portal CyberMaps.ru.

Keywords: cyber polygon, information map, information mapping, artificial intelligence, machine learning.

DOI 10.36622/VSTU.2023.26.2.007
УДК 004.056.55/003.26

ЭВОЛЮЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТ ЗАЩИТЫ ДАННЫХ И ИНФОРМАЦИИ К ЗАЩИТЕ ЗНАНИЙ – НАУКОМЕТРИЧЕСКИЕ АСПЕКТЫ (Часть II)

П.Ю. Филяк

Проблема информационной безопасности никогда не утрачивала своей актуальности по мере развития современного общества, а в условиях глобализации становления и распространения информационного общества и выхода его на новый качественный уровень становится особенно острой. Тем более, с учетом такого объективного фактора как бурное, динамичное и повсеместное внедрение во всех сферах жизни такого, относительно нового явления, как искусственный интеллект, который становится непреложным условием технического и технологического прогресса человечества. Как известно, человеческая цивилизация находится на пороге нового технологического скачка и остро нуждается в получении качественно новых знаний, выхода на новый качественный уровень, что подразумевает и предполагает появление в ближайшее время открытий в разных научных сферах и прежде всего в фундаментальной науке, точных и естественных науках. Задача скорейшего получения новых знаний и, особенно, принципиально новых знаний на настоящий момент встала необыкновенно остро. Для получения новых знаний необходимо использование новых подходов и инструментов, к каковым относится и искусственный интеллект, - многоплановый и эффективный, но и на настоящий момент относительно неизученный с точки зрения возможных негативных последствий бесконтрольного его применения. Поэтому задача обеспечения информационной безопасности переходит из плоскости своей актуальности на новый качественный уровень.

Ключевые слова: информация, данные, знания, мудрость, концепция DIKW, наукометрия, науковедение, искусственный интеллект, информационная безопасность, инвестиции в науку, чат-боты, платформы искусственного интеллекта.

THE EVOLUTION OF INFORMATION SECURITY – FROM DATA AND INFORMATION PROTECTION TO KNOWLEDGE PROTECTION – SCIENTOMETRIC ASPECTS (Part II)

P.Yu. Filyak

The problem of information security has never lost its relevance with the development of modern society, and in the context of globalization, the formation and spread of the information society and its entry into a new qualitative level becomes especially acute. Moreover, taking into account such an objective factor as the rapid, dynamic and widespread introduction in all spheres of life of such a relatively new phenomenon as artificial intelligence, which becomes an indispensable condition for the technical and technological progress of mankind. As you know, human civilization is on the threshold of a new technological leap and is in urgent need of obtaining qualitatively new knowledge, reaching a new qualitative level, which implies and assumes the appearance in the near future of discoveries in various scientific fields and, above all, in fundamental science, exact and natural sciences. The task of obtaining new knowledge as soon as possible and, especially, fundamentally new knowledge has become extremely acute at the moment. To gain new knowledge, it is necessary to use new approaches and tools, which include artificial intelligence, which is multifaceted and effective, but also relatively unexplored at the moment in terms of possible negative consequences of its uncontrolled use. Therefore, the task of ensuring information security is moving from the plane of its relevance to a new qualitative level.

Keywords: information, data, knowledge, wisdom, DIKW concept, scientometrics, science studies, artificial intelligence, information security, investments in science, chatbots, artificial intelligence platforms.

DOI 10.36622/VSTU.2023.26.2.008
УДК 004.056.57

АТАКИ ТИПА «СЕТЕВАЯ РАЗВЕДКА»: РИСК-ЛАНДШАФТ И ЧАСТНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

А.Ю. Пекло, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко

В работе рассматривается специфика построения частной политики в части защиты сети предприятия от сетевой разведки в соответствии с риск-ландшафтом. Сформировано полное множество сценариев и уязвимостей сетевой разведки. На основании статистики, частоты и ущербности атак выявлены наиболее опасные сочетания сценариев и уязвимостей заданного типа атаки. Построен риск-ландшафт реализации сетевой разведки. В результате предлагается специфика частной политики защиты сети организации от сетевой разведки, учитывающая наиболее опасные сочетания векторов и уязвимостей заданного типа атаки. Предложенная специфика может быть использована для разработки внутренних документов организации, в которых содержатся детальные разъяснения положений по защите сети от разведывательных действий со стороны киберзлоумышленника.

Ключевые слова: сетевая разведка, уязвимость, сценарий атаки, риск-ландшафт, частная политика.

ATTACKS SUCH AS «NETWORK RECONNAISSANCE»: RISK LANDSCAPE AND PRIVATE INFORMATION SECURITY POLICY

A.Yu. Peklo, G.A. Ostapenko, D.V. Shcherbakova, A.A. Ostapenko

The article considers the specifics of building a private policy in terms of protecting the enterprise network from network exploration in accordance with the risk landscape. A complete set of network intelligence scenarios and vulnerabilities has been formed. Based on statistics, frequency and flaw, the most dangerous combinations of scenarios and vulnerabilities of a given type of attack were identified. A risk landscape for the implementation of network intelligence has been built. As a result, the specifics of private policy are proposed in terms of protecting an enterprise's network from network intelligence, taking into account the most dangerous combinations of vectors and vulnerabilities of a given type of attack. The proposed specifics can be used to develop internal documents of the organization, which contain detailed explanations of the provisions for the protection of the network from intelligence actions by a cyber attacker.

Keywords: network reconnaissance, vulnerability, attack scenario, risk landscape private enterprise security policy.

DOI 10.36622/VSTU.2023.26.2.009
УДК 004.048

БАЗА ДАННЫХ КОНТЕНТОВ С ПРИЗНАКАМИ ДЕСТРУКТИВНОСТИ

Е.Ю. Чапурин, Н.М. Лантюхов, П.Д. Федоров, А.О. Феоктистов, А.Ю. Егоров

Статья посвящена созданию базы данных для хранения информации о выявленных деструктивных контентах, созданию математического обеспечения для поиска, аналитики и визуализации результатов работы с созданной базой данных. При помощи разработанного математического аппарата для созданной базы данных существует возможность поиска и анализа контентов с признаками деструктивности на любых информационных ресурсах. Структура базы данных, позволяет хранить информацию о контенте любого типа. Разработано программное обеспечение, позволяющее автоматизировать работу с синтезированной базой данных. Разработанный программный комплекс применим для организации процесса риск-анализа и позволяет минимизировать затрачиваемое время, автоматизировать некоторые части данного процесса, а также организовать простое и понятное взаимодействие пользователя с защищенной базой данных контентов деструктивного характера. Полученные результаты могут быть использованы для проведения подробного процесса риск-анализа контентов и пользовательских комментариев, что поможет создать более детальные механизмы обеспечения безопасности конкретного пользователя и профилактики эпидемий в социальных сетях. На основе предложенного программного комплекса существует возможность реализовать механизм модерации контента до его фактической публикации на информационных ресурсах.

Ключевые слова: база данных, деструктивный контент, социальная сеть.

DATABASE OF CONTENT WITH SIGNS OF DESTRUCTIVENESS

E.Yu. Chapurin, N.M. Lantyukhov, P.D. Fedorov, A.O. Feoktistov, A.Yu. Egorov

The article is devoted to the creation of a database for storing information about the identified destructive content, the creation of mathematical software for search, analytics and visualization of the results of work with the created database. With the help of the developed mathematical apparatus for the created database, it is possible to search and analyze content with signs of destructiveness on any information resources. The database structure allows you to store information about any type of content. The software allowing to automate work with the synthesized database is developed. The developed software package is applicable to the organization of the risk analysis process and allows you to minimize the time spent, automate some parts of this process, as well as organize a simple and understandable user interaction with a secure database of destructive content. The results obtained can be used to conduct a detailed process of risk analysis of content and user comments, which will help create more detailed mechanisms to ensure the safety of a particular user and prevent epidemics in social networks. Based on the proposed software package, it is possible to implement a mechanism for content moderation before its actual publication on information resources.

Keywords: database, destructive content, social networks.

DOI 10.36622/VSTU.2023.26.2.010
УДК 004.056.57

СЕТЕВЫЕ АТАКИ НА УРОВНЕ ПРИЛОЖЕНИЙ: РИСК-ЛАНДШАФТ И ЧАСТНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

С.А. Хромых, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко

Рассмотрена проблема сетевых атак на уровне приложений и обосновывается её актуальность. Приведены векторы и уязвимости сетевых атак на уровне приложений. Описана и реализована методика риск-оценки на основе данных по атакам и уязвимостям в 2022 году. Построены матрица уязвимостей и риск-ландшафт по данным риск-оценок в указанном периоде. На основе риск-ландшафта проведена оценка степени опасности векторов атак и уязвимостей. Выделены наиболее опасные сочетания векторов и уязвимостей. Для таких сочетаний предложение соответствующие фрагменты частной политики защиты информации. Акцентируется внимание на важности разработки частных политик безопасности информации, учитывающих особенности деятельности конкретных предприятий для более эффективной защиты от атак на уровне приложений и не только.

Ключевые слова: корпоративная сеть, векторы атаки, уязвимости, риск-ландшафт, частная политика.

NETWORK ATTACKS AT THE APPLICATION LEVEL: RISK LANDSCAPE AND PRIVATE INFORMATION SECURITY POLICY OF THE ENTERPRISE

S.A. Khromykh, G.A. Ostapenko, D.V. Shcherbakova, A.A. Ostapenko

The problem of network attacks at the application level is considered and its relevance to this problem is substantiated. Vectors and vulnerabilities of network attacks at the application level are given. A risk assessment methodology based on data on attacks and vulnerabilities in 2022 is described and implemented. A vulnerability matrix and a risk landscape are built based on risk assessment data in the specified period. Based on the risk landscape, the degree of danger of attack vectors and vulnerabilities is assessed. The most dangerous combinations of vectors and vulnerabilities are highlighted. For such combinations, corresponding fragments of a private information protection policy are proposed. Attention is focused on the importance of developing private information security policies that take into account the specifics of the activities of specific enterprises for more effective protection against attacks at the application level and beyond.

Keywords: attack vectors, vulnerabilities, risk landscape, private policy.

DOI 10.36622/VSTU.2023.26.2.011
УДК 004.056

БИОМЕТРИЯ ПАРОЛЬНОГО ВВОДА: НОВАЯ МОДЕЛЬ АУТЕНТИФИКАЦИИ

В.А. Минаев, **И.С. Стручков**

В статье рассматривается возможность усиления метода аутентификации сочетанием пароля и клавиатурного почерка пользователя на входе в компьютерную систему. Для обоснования новой биометрической модели аутентификации рассматриваются результаты экспериментов по замерам забывания информации, полученные в XIX веке немецким психологом Г. Эббингаузом. Выдвигается и проверяется гипотеза, что процесс ввода пользователем пароля с клавиатуры характеризуется кривой экспоненциального типа, когда вначале время скорость ввода минимальна, соответственно, время ввода – максимально, а затем по мере новых повторений скорость ввода увеличивается, а время ввода уменьшается, стремясь к некоторому пределу. При этом для каждого пользователя наблюдаются характерные только ему параметры экспоненциальной кривой. Для построения модели клавиатурного почерка с 30 участниками проведены эксперименты по изучению его динамических параметров. Мерой соответствия между теоретической и экспериментальной кривой, а также критерием аутентификации пользователя служит значение коэффициента детерминации R^2. Анализ результатов моделирования показал, что участники эксперимента делятся на три типологические группы в пространстве параметров клавиатурного почерка. Группы значимо различаются гендерными и психологическими признаками, отражающими типохарактер пользователя.

Ключевые слова: биометрический метод, аутентификация, клавиатурный почерк, кривая забывания, математическая модель, типология.

PASSWORD ENTRY BIOMETRICS: NEW AUTHENTICATION MODEL

V.A. Minaev, **I.S. Struchkov**

The article discusses the possibility of strengthening the authentication method by combining a password and a user's keyboard handwriting at the entrance to a computer system. To substantiate the new biometric authentication model, the results of experiments on measurements of forgetting information obtained in the XIX century by the German psychologist G. Ebbinghaus are considered. The hypothesis is put forward and tested that the process of entering a password by the user from the keyboard is characterized by an exponential curve, when at first the input speed is minimal, respectively, the input time is maximal, and then as new repetitions occur, the input speed increases and the input time decreases, tending to a certain limit. At the same time, for each user, the exponential curve parameters characteristic only of him are observed. To build a model of keyboard handwriting, experiments were conducted with 30 participants to study its dynamic parameters. The value of the determination coefficient R2 serves as a measure of the correspondence between the theoretical and experimental curve, as well as the user authentication criterion. Analysis of the simulation results showed that the participants of the experiment are divided into three typological groups in the space of keyboard handwriting parameters. The groups differ significantly in gender and psychological characteristics reflecting the type of character of the user.

Keywords: biometric method, authentication, keyboard handwriting, information forgetting curve, mathematical model, typology.

DOI 10.36622/VSTU.2023.26.2.012
УДК 004.056.47

СОЗДАНИЕ КИБЕРПОЛИГОНА: ФОРМИРОВАНИЕ БЛОКА ЭМУЛЯЦИИ И СКАНИРОВАНИЯ ИНФРАСТРУКТУРЫ

С.С. Куликов, А.И. Саушкин

В работе предлагается вариант реализации программно-технического комплекса (ПТК), являющегося блоком анализа безопасности киберполигона. Блок позволяет эмулировать инфраструктуру заказчика и проводить ее сканирование на предмет наличия уязвимостей. Компонент эмуляции инфраструктуры обеспечивает ее быструю инициализацию и, при необходимости, оперативное восстановление. За счет использования технологий, обеспечивающих быстрое развертывание, инфраструктура может быть поднята на различных вычислительных ресурсах. Компонент анализа защищенности позволяет пользователю провести сканирование инфраструктуры на наличие уязвимостей и получить подробную информацию о них. Чтобы обеспечить прозрачную для пользователя интеграцию компонентов блока и простоту его использования реализовано специальное приложение, выполняющее роль пользовательского интерфейса. ПТК позволяет реализовать различные способы размещения его компонентов даже на менее ресурсообеспеченных платформах за счет использования технологий контейнеризации.

Ключевые слова: киберполигон, информационная безопасность, эмуляция, технология быстрого развертывания.

CREATION OF A CYBERPOLYGON: FORMATION OF THE UNIT OF EMULATION AND SCANNING OF INFRASTRUCTURE

S.S. Kulikov, A.I. Saushkin

The paper proposes an implementation option for a software and hardware complex (SHC), which is a block for analyzing the security of a cyberpolygon. The block allows you to emulate the customer's infrastructure and scan it for vulnerabilities. The infrastructure emulation component ensures its quick initialization and, if necessary, quick recovery. Through the use of technologies that provide rapid deployment, the infrastructure can be raised on various computing resources. The security analysis component allows the user to scan the infrastructure for vulnerabilities and obtain detailed information about them. To ensure transparent integration of the block components for the user and ease of use, a special application has been implemented that acts as a user interface. SHC allows you to implement various ways of placing its components even on less resource-provided platforms through the use of containerization technologies

Keywords: cyberpolygon, information security, emulation, rapid deployment technology.

DOI 10.36622/VSTU.2023.26.2.013
УДК 004.056.47

СОЗДАНИЕ КИБЕРПОЛИГОНА: ФОРМИРОВАНИЕ БЛОКА СИМУЛЯЦИИ

С.С. Куликов, В.К. Федоров

В настоящей статье описаны особенности разработки и реализации блока симуляции киберполигона, предназначенного для проведения тренировок и аудита кибербезопасности. В рамках работы были проанализированы существующие реализации киберполигонов, основные принципы их функционирования, на основе чего был определен подход к моделированию и реализован соответствующий программный блок симуляции. Реализованный программно-технический комплекс (ПТК) позволяет динамически наполнять инфраструктуру, отображать сетевые топологии в виде динамического графа. Также предусмотрено формирование отчётов по найденным уязвимостям и эксплойтам. Работа с блоком симуляции осуществляется посредством использования веб-страницы, функционал которой позволяет: добавлять узлы, изменять топологию сети, запускать сетевое сканирование и формировать отчёт безопасности. Гибкость ПТК достигается применением микросервисной архитектуры совместно с технологией контейнеризации. Экспериментальные результаты показывают, что акцент на симуляцию процессов, а также графовое представление инфраструктуры позволяет не только повысить уровень осведомленности в сфере информационной безопасности (ИБ), но и эффективно выявлять и анализировать уязвимости, прогнозировать потенциальные угрозы от действий злоумышленников и принимать соответствующие меры для защиты информационных систем.

Ключевые слова: киберполигон, граф, уязвимость, эксплойт.

CREATING A CYBER POLYGONE: GENERATING A SIMULATION BLOCK

S.S. Kulikov, V.K. Fedorov

This article describes the development and implementation of a cyber-polygon simulation unit designed for cybersecurity training and testing. As part of the work, the following were considered: a set of domestic implementations of cyber polygons, the basic principles of their functioning, an approach to its modeling was chosen, and an appropriate simulation software block was implemented. The implemented software and hardware complex allows you to dynamically fill the infrastructure, display network topologies in the form of a graph. It also provides for the generation of reports on found vulnerabilities and exploits. Working with the simulation block is carried out through the use of a web page where you can: add nodes, change the network topology, run a network scan and analyze the security report. The flexibility of the software and hardware complex is achieved by using a microservice architecture coupled with containerization technology. Experimental results have shown that the emphasis on process simulation, as well as graph manipulation, allows not only to increase the level of information security awareness, but also to effectively identify and analyze vulnerabilities, predict potential threats from the actions of intruders and take appropriate countermeasures to protect information systems.

Keywords: cyber polygons, graphs, vulnerabilities, exploits.