DOI 10.36622/VSTU.2023.26.3.015
УДК 004.056

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ МЕНТАЛЬНО-КОГНИТИВНЫХ ВОЙН

А.С. Овчинский

В статье отмечается изменение и развитие представлений об информационной безопасности на этапах автоматизации, цифровизации и цифровой трансформации. Акцентируется внимание на угрозах социальным сферам, которые связаны с деструктивными воздействиями на сознание людей, сообществ, народов. Вводится понятие глубинной, пролонгированной информационной войны. Ее ментальные, когнитивные и смысловые направления раскрываются в системе координат реактивной, ресурсной и фоновой информации. Сама информация рассматривается как инструмент и основное оружие современной психо-демографической, психо-исторической и идеологической войны.

Ключевые слова: информационная безопасность, социальные сферы, ментальная война, когнитивная война, смысловая война, психо-демографическая война, психо-историческая война, идеологическая война, мировые идеологии, информационные координаты.

THREATS TO INFORMATION SECURITY IN THE CONTEXT OF MENTAL AND COGNITIVE WARS

A.S. Ovchinsky

The article discusses the change and development of ideas about information security at the stages of automation and digital transformation. Attention is focused on threats to social spheres that are associated with destructive effects on the consciousness of people and communities. The concept of deep, prolonged information warfare is introduced. Its mental, cognitive and semantic directions are revealed in the coordinate system of reactive, resource and background information. The information considered as a tool and the main weapon of modern psycho-demographic, psycho-historical and ideological warfare.

Keywords: information security, social spheres, mental war, cognitive war, semantic war, psycho-demographic war, psycho-historical war, ideological war, world ideologies, information coordinates.

DOI 10.36622/VSTU.2023.26.3.016
УДК 004.056

МЕТОДЫ БИОМАРКИРОВАНИЯ ЗАЩИЩАЕМЫХ ОБЪЕКТОВ

В.А. Минаев, С.В. Дворянкин, А.М. Алюшин

В статье для совершенствования технологий подтверждения валидности документов рассматривается комплексный подход использования биометрической подписи для бумажной и электронной форм хранения и передачи данных. Сравниваются методы электронной и речевой подписи, при этом последняя рассматривается в качестве носителя наиболее важной контекстной информации защищаемого документа, так и индивидуальных биометрических характеристик автора. Для этой цели предусмотрена передача в составе биоподписи информации о состоянии сердечно-сосудистой, нервной и дыхательной системы автора. Показано, что указанные дополнительные биопараметры позволяют значительно повысить достоверность оценки текущего функционального и психоэмоционального состояния автора документа. Применение технологии биомаркирования позволяет выявлять случаи неадекватного состояния, а также факты принуждения к подписи и утверждению документа. Значение интегрированного показателя качества разработанных алгоритмических и программных средств подтверждения валидности документов за счет использования биоподписи составило 99,4%. Сравнение биоподписи с речевой подписью показало выигрыш первой на 46%.

Ключевые слова: валидность документа, биометрическая подпись, параметры сердечно-сосудистой, нервной, дыхательной систем, интегрированный показатель.

METHODS OF BIOMARKING PROTECTED OBJECTS

A.M. Alyushin, S.V. Dvoryankin, V.A. Minaev

The article considers a comprehensive approach to using biometric signatures for paper and electronic forms of data storage and transmission in order to improve the technologies for confirming the validity of documents. The methods of electronic and speech signatures are compared, while the latter is considered as the carrier of the most important contextual information of the protected document, as well as the individual biometric characteristics of the author. For this purpose, the transfer of information about the state of the author's cardiovascular, nervous and respiratory system as part of the bio-signature is provided. It is shown that these additional bioparameters can significantly increase the reliability of the assessment of the current functional and psycho-emotional state of the author of the document. The use of biomarking technology makes it possible to identify cases of inadequate condition, as well as facts of coercion to sign and approve a document. The value of the integrated quality indicator of the developed algorithmic and software tools for confirming the validity of documents through the use of bio-signatures was 99.4%. A comparison of a bio-signature with a speech signature showed a 46% gain for the first one.

Keywords: validity of the document, biometric signature, state of the cardiovascular, nervous, respiratory systems, integrated indicator.

DOI 10.36622/VSTU.2023.26.3.017
УДК 004.056

ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА ОТ СЕТЕВЫХ АТАК: МЕТОДИКИ ФОРМИРОВАНИЯ ЧАСТНЫХ ПОЛИТИК, РЕГЛАМЕНТОВ И ИНСТРУКЦИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (ЧАСТЬ I)

Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.С. Кривошеин

Предлагается методическое обеспечение для формирования частных политик защиты корпоративной сети. Представляемая методология построения частной политики разрабатывается на основании лучших практик и рекомендаций в области информационной безопасности, также учитывает окна, позволяющие адаптировать частную политику под специфику различных атак. Частная политика определяет основные цели и задачи организации в части противодействия сетевым атакам, задает основное направление в развитии структуры взаимоувязанных документов, таких как частные регламенты и инструкции сетевой безопасности. Разрабатывается план по формированию перечня мероприятий, включающий в себя требования и меры по защите информации с учетом специфики сетевой атаки. Производится разграничение зон ответственности по вопросам обеспечения безопасности должностных лиц и описываются методы и средства контроля за реализацией требований, определенных частной политикой.

Ключевые слова: частная политика, сетевая атака, меры защиты, объекты защиты, модель нарушителя.

ORGANIZATIONAL AND LEGAL PROTECTION AGAINST NETWORK ATTACKS: METHODS FOR FORMING PRIVATE POLICIES, REGULATIONS AND INSTRUCTIONS TO ENSURE ORGANIZATION SECURITY (PART I)

G.A. Ostapenko, D.V. Shcherbakova, T.Yu. Miroshnichenko, A.A. Ostapenko, A.S. Krivoshein

Proposed methodological support for the formation of private policies to protect the corporate network. The presented methodology for building a private policy is developed on the basis of best practices and recommendations in the field of information security, and also takes into account windows that allow you to adapt a private policy to the specifics of various attacks. Private policy defines the main goals and objectives of the organization in terms of countering network attacks, sets the main direction in the development of the structure of interrelated documents, such as private regulations and instructions for network security. A plan is being developed to form a list of measures, which includes requirements and measures for protecting information, taking into account the specifics of a network attack. The areas of responsibility for ensuring the security of officials are delineated and the methods and means of monitoring the implementation of the requirements defined by private policy are described.

Keywords: private policy, network attack, protection measures, objects of protection, intruder model.

DOI 10.36622/VSTU.2023.26.3.018
УДК 004.056

ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА ОТ СЕТЕВЫХ АТАК: МЕТОДИКИ ФОРМИРОВАНИЯ ЧАСТНЫХ ПОЛИТИК, РЕГЛАМЕНТОВ И ИНСТРУКЦИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (ЧАСТЬ II)

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

Предлагается методическое обеспечение для формирования частных регламентов защиты корпоративных сетей. Представляемая методология создания частных регламентов направлена на процесс управления инцидентами нарушения безопасности, возникающие вследствие реализации различных типов сетевых атак. Частные регламенты включают в себя: регламент обнаружения и регистрации инцидентов нарушения сетевой безопасности, регламент реагирования на инциденты нарушения сетевой безопасности, регламент ликвидации последствий инцидентов нарушения сетевой безопасности. Приведенная методика по построению регламентов позволяет классифицировать инциденты нарушения безопасности, учитывая их уровень критичности и приоритет, также определяет механизмы регистрации. Представлен алгоритм по реагированию на инциденты и по выявлению и ликвидации негативных последствий, вызванных инцидентами.

Ключевые слова: частные регламенты, сетевая атака, инцидент безопасности, события безопасности.

ORGANIZATIONAL AND LEGAL PROTECTION AGAINST NETWORK ATTACKS: METHODS FOR FORMING PRIVATE POLICIES, REGULATIONS AND INSTRUCTIONS TO ENSURE ORGANIZATION SECURITY (PART II)

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

Proposed methodological support for the formation of private regulations for the protection of corporate networks of the organization. The presented methodology for creating private regulations is aimed at managing incidents of security breaches arising from the implementation of various types of network attacks. Private regulations include: the regulation for detecting and registering incidents of network security violations, the regulation for responding to incidents of network security violations, the regulation for eliminating the consequences of incidents of network security violations. The above methodology for the construction of regulations allows classifying security breach incidents, taking into account their level of criticality and priority, and also determines the registration mechanisms. An algorithm for responding to incidents and for identifying and eliminating the negative consequences caused by incidents is presented.

Keywords: private regulations, network attack, security incident, security events.

DOI 10.36622/VSTU.2023.26.3.019
УДК 004.056

ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА ОТ СЕТЕВЫХ АТАК: МЕТОДИКИ ФОРМИРОВАНИЯ ЧАСТНЫХ ПОЛИТИК, РЕГЛАМЕНТОВ И ИНСТРУКЦИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (ЧАСТЬ III)

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

Предлагается методическое обеспечение для формирования частных инструкций защиты корпоративной сети. Частные инструкции включают в себя: инструкцию администратора безопасности и инструкцию внутреннего и внешнего пользователя. Предложенная методика построения инструкции администратора безопасности определяет основные требования к его должностным обязанностям. Проработаны рекомендации в части выбора и настройки средств защиты информации, необходимых и достаточных для защиты при сетевой атаке заданного типа. Также представлен план по построению разграничительной матрицы доступа, которая позволяет обеспечить защиту от несанкционированного доступа и каких-либо преднамеренных ошибок пользователей. Представленная структура инструкции пользователя регламентирует его безопасную работу, также определяет план обучения и инструктирования, который позволит повысить грамотность пользователей в части защиты информации.

Ключевые слова: частные инструкции, сетевая атака, администратор безопасности, пользователь.

ORGANIZATIONAL AND LEGAL PROTECTION AGAINST NETWORK ATTACKS: METHODS FOR FORMING PRIVATE POLICIES, REGULATIONS AND INSTRUCTIONS TO ENSURE ORGANIZATION SECURITY (PART III)

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

Proposed methodological support for the formation of private instructions for the protection of the corporate network. Private instructions include: security administrator instruction and internal and external user instruction. The proposed methodology for constructing instructions for a security administrator defines the basic requirements for his job responsibilities. Recommendations have been worked out regarding the selection and configuration of information protection tools that are necessary and sufficient to protect against a network attack of a given type. A plan is also presented for building a delimiting access matrix, which allows you to provide protection against unauthorized access and any deliberate user errors. The presented structure of the user manual regulates its safe operation, and also defines a training and instruction plan that will increase the literacy of users in terms of information protection.

Keywords: private instructions, network attack, security administrator, user.

DOI 10.36622/VSTU.2023.26.3.020
УДК 004.056.55/003.26

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

П.Ю.Филяк

В настоящее время, с учетом всё более глубокого вхождения ведущих мировых держав в информационное общество, индикатором чего является необратимое развитие цифровой экономики и прежде всего в наиболее развитых странах, что в качестве стратегической цели было обозначено еще в январе 2016 года на Всемирном экономическом форуме в Давосе Клаусом Швабом как «Четвертая промышленная революция», или Индустрия 4.0, становится абсолютно очевидным, что информационные технологии, в частности, становятся основным его локомотивом. На базе информационных технологий будет применяться и уже широко применяется целый спектр разнообразных новых инструментов, одним из эффективнейших среди которых является искусственный интеллект (ИИ/AI). Но ИИ при всех его возможностях и значимости является всего лишь инструментом Индустрии 4.0 – нового технологического уклада, а основой, инвариантным базисом являются и будут являться знания, в том числе принципиально новые знания, которые повлекут за собой открытия во всех областях, практически без исключения, и прежде всего в естественных (точные науки – физика, математика) и инженерно-технических науках. Знания, согласно концепции Рассела Акоффа, как известно, являются одной из страт пирамиды DIKW, стоящей над информацией и добавляющей по отношению к категории информация механизм её использования, отвечая на вопрос «как?», поэтому они должны предусматривать защиту еще большую, чем информация, как категория более ценная. И требования по защите знаний должны быть на порядок выше требований по защите информации и информационной безопасности.

Ключевые слова: данные, информация, знания, мудрость, концепция DIKW, науковедение, наукометрия, искусственный интеллект, информационная безопасность, псевдознания, псевдонауки, гуманитарные аспекты информационной безопасности.

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

P.Yu.Filyak

At present, taking into account the ever deeper entry of the leading world powers into the information society, the indicator of which is the irreversible development of the digital economy, especially in the most developed countries, which was designated as a strategic goal back in January 2016 at the World Economic Forum in Davos by Klaus Schwab as the "Fourth Industrial Revolution", or Industry 4.0, it becomes absolutely obvious that information technology, in particular, is becoming its main locomotive, on the basis of information technologies, a whole range of various new tools will be used and is already widely used, one of the most effective among which is artificial intelligence (AI). But AI, with all its capabilities and significance, is just a tool of Industry 4.0 – a new technological order, and the basis, the invariant basis is and will be knowledge, including fundamentally new knowledge that will entail discoveries in all fields, almost without exception, and above all in natural sciences (exact sciences – physics, mathematics) and engineering and technical sciences. Knowledge, according to the concept of Russell Akoff, is known to be one of the strata of the DIKW pyramid, standing above information and adding a mechanism for its use in relation to the information category, answering the question "how?", therefore they should provide even greater protection than information, as a more valuable category. And the requirements for the protection of knowledge should be an order of magnitude higher than the requirements for the protection of information and information security.

Keywords: data, information, knowledge, wisdom, DIKW concept, science studies, scientometry, artificial intelligence, information security, pseudo knowlege, pseudo science, humanitarian aspects of information security.

DOI 10.36622/VSTU.2023.26.3.021
УДК 004.45

КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С ПОВЫШЕНИЕМ ПРИВИЛЕГИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НА БАЗЕ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА LINUX, И ОЦЕНКА РИСКОВ ИХ ЭКСПЛУАТАЦИИ

А.Л. Сердечный, И.А. Каданцев Д.И. Лоскутов

В работе проведена оценка и регулирование рисков для автоматизированных систем, связанных с возможностью повышения привилегий в операционных системах семейства Linux. Проведена классификация уязвимостей, связанных с повышением привилегий в автоматизированных системах на базе операционных систем семейства Linux, с учётом возможности количественного оценивания рисков, возникающих в результате эксплуатации таких уязвимостей. Предложена методика оценки рисков рассматриваемых рисков. Данная методика разработана на основе преобразования качественных метрик стандарта CVSS в количественные метрики, направленные на определение вероятности эксплуатации уязвимости и степени ущерба автоматизированной системе на базе операционной системы семейства Linux.

Ключевые слова: операционная система Linux, повышение привилегий, риск, уязвимость, повышение защищенности автоматизированной системы.

ASSESSMENT AND REGULATION OF RISKS FOR AUTOMATED SYSTEMS ASSOCIATED WITH THE POSSIBILITY OF PRIVILEGE ESCALATION IN LINUX OPERATING SYSTEMS

A.L. Serdechnyy, I.A. Kadantsev, D.I. Loskutov

In this article the assessment and management of risks for automated systems associated with the possibility of privilege escalation in operating systems of the Linux family were carried out. A classification of vulnerabilities related to privilege escalation in automated systems based on Linux operating systems has been made, taking into account the possibility of quantitatively assessing the risks arising from the exploitation of such vulnerabilities. A method for assessing the risks of the risks under consideration is proposed. This method was developed based on converting the qualitative metrics of the CVSS standard into quantitative metrics aimed at determining the possibility of vulnerability exploitation and the degree of damage to an automated system based on the Linux operating system.

Key words: Linux operating system, privilege escalation, risk, vulnerability, increased security of an automated system. Suggestions was given for using this technique to assess the risks of exploiting vulnerabilities in more complex data structures.

DOI 10.36622/VSTU.2023.26.3.022
УДК 004.056

НАУЧНО-ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ КАФЕДРЫ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ПРОГРАММЫ «КИБЕРПОЛИГОН»

А.Г. Остапенко, С.С. Куликов, А.А. Остапенко, Е.А. Москалева, Е.С. Петрова

Обучение современных специалистов в вузе требует активного участия студентов в проектной деятельности и научной деятельности кафедр. Требования со стороны работодателей и Минобразования неуклонно усложняются ввиду стремительного технического прогресса. Это приводит к необходимости формирования новых методов и подходов к обучению со стороны профессорско-преподавательского состава вуза. В 2022/2023 учебном году кафедра систем информационной безопасности Воронежского государственного технического университета успешно осуществила работу по созданию и внедрению в учебную деятельность студентов и аспирантов киберполигона. В статье предложена организация проектной и научной деятельности кафедры информационной безопасности на основе киберполигона и изложены организационные и правовые мероприятия для его функционирования.

Ключевые слова: киберполигон, кибердружина, информационная безопасность, организационно-правовое обеспечение программы, дорожная карта программы, проектная деятельность кафедры.

SCIENTIFIC AND PROJECT ACTIVITY OF THE DEPARTMENT OF INFORMATION SECURITY SYSTEMS WITHIN "CYBER TRAINING GROUND" PROGRAM

A.G. Ostapenko, S.S. Kulikov, A.A. Ostapenko, E.A. Moskaleva, E.S. Petrova

Training modern specialists at a university requires the active participation of students in project activities and scientific activities of departments. Requirements from employers and the Ministry of Education are steadily becoming more complex due to rapid technological progress. This leads to the need for the formation of new methods and approaches to learning on the part of the teaching staff of the university. In the 2022/2023 academic year, the Department of Information Security Systems of the Voronezh State Technical University successfully carried out work to create and implement a cyber training ground in the educational activities of students and postgraduates. The article proposes the organization of project and scientific activities of the Department of Information Security on the basis of a cyber training ground and outlines organizational and legal measures for its functioning.

Keywords: cyber training ground, cyber squad, information security, organizational and legal support of the program, program roadmap, project activities of the department.

DOI 10.36622/VSTU.2023.26.3.023
УДК 004.056

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ: НАУЧНО-ПРАКТИЧЕСКИЕ РЕАЛИИ И ГОРИЗОНТЫ

Д.В. Щербакова

В работе рассматриваются вопросы защиты корпоративных сетей. В этой связи осуществлено целеполагание данного исследования с акцентом на организационно-правовые аспекты. Предлагается методическое обеспечение борьбы с сетевыми вторжениями через риск-формализацию деятельности корпоративных сетей в части формирования адекватных атакам политик, регламентов и инструкций защищаемых организаций. Особое внимание уделяется формированию сетевой контрразведки, ибо все современные атаки предварительно готовятся на основе данных, полученных в ходе реализации сетевых разведывательных действий. В этой связи предлагаются формы соответствующей регламентации. Рассматриваются концепция, функционал и архитектура корпоративного полигона как тренажера персонала организации в ходе сетевого противоборства.

Ключевые слова: безопасность, корпоративная сеть, политика безопасности, регламент безопасности, инструкции безопасности, сетевая контрразведка, киберполигон.

ORGANIZATIONAL AND LEGAL ASPECTS OF PROTECTION OF CORPORATE NETWORKS: SCIENTIFIC AND PRACTICAL REALITIES AND HORIZONS

D.V. Shcherbakova

The work discusses the protection of corporate networks. In this regard, the goal of this study was carried out with an emphasis on organizational and legal aspects. Methodological support for the fight against network invasions through the risk of the activities of corporate networks in terms of the formation of an adequate politician, regulations and instructions of protected organizations. Particular attention is paid to the formation of network counterintelligence, because all modern attacks are pre - prepared on the basis of data obtained during the implementation of network intelligence actions. In this regard, forms of appropriate regulation are proposed. The concept, functionality and architecture of the corporate training ground as a simulator of the organization's personnel during a network confrontation are considered.

Keywords: security, corporate network, security policy, security regulations, safety instructions, network counterintelligence, cyberpolygon.

DOI 10.36622/VSTU.2023.26.3.024
УДК 004.056

НЕЙРОСЕТЕВАЯ МОДЕЛЬ ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

С.А. Ермаков, А. Г. Чурсин, П.А. Анцупов

Разработана модель обнаружения сетевых вторжений, с использованием нейросетевых структур, главным отличием которой является более точная идентификация угроз, по сравнению с аналогами. Проанализированы публикации по темам выявления угроз информационной безопасности, особенностям применения машинного обучения и эффективности использования моделей нейронных сетей с глубоким обучением для обнаружения атак. Выделены нерешенные частные проблемы, требующие детальной проработки: выбор наиболее оптимальной архитектуры нейронной сети, и комбинирование методов статистического анализа и машинного обучения. Представлена модель системы обнаружения вторжений и вредоносной активности, которая сочетает в себе аналитику поведения пользователей и модель выявления аномалий. Предложенная модель позволяет отслеживать кибератаки, для которых отсутствуют сигнатуры, и снизить уровень ложных срабатываний при идентификации ранее неизвестных кибератак.

Ключевые слова: атака, информационная система, нейронная сеть, пользователь.

NEURAL NETWORK MODEL FOR IMPROVING THE ACCURACY OF NETWORK INTRUSION DETECTION

S.A. Ermakov, A. G. Chursin, P.A. Antsupov

A model for detecting network intrusions using neural network structures has been developed, the main difference of which is a more accurate identification of threats compared to analogues. Analyzed publications on the topics of identifying information security threats, the specifics of using machine learning and the effectiveness of using neural network models with deep learning to detect attacks. The unsolved parts requiring detailed study are highlighted: the choice of the most optimal neural network architecture, and the combination of statistical analysis and machine learning methods. A model of an intrusion detection system and malicious activity is presented, which combines user behavior analytics and an anomaly detection model. The proposed model allows you to track cyber-attacks for which there are no signatures and reduce the level of false positives when identifying previously unknown cyber-attacks.

Keywords: attack, information system, neural network, user.

DOI 10.36622/VSTU.2023.26.3.025
УДК 004.056.55/003.26

БЕЗОПАСНОСТЬ ЗНАНИЙ ПРИ ИСПОЛЬЗОВАНИИ ЧАТ-БОТОВ GPT

П.Ю. Филяк, А.Н.Дымов, К.П.Колпаков

Рассматривается информационная безопасность в эпоху Индустрии 4.0 через призму концепции Рассела Акоффа – знаменитой пирамиды DIKW, в которой знания, как известно, являются одной из страт данной пирамиды, вышестоящей над информацией и добавляющей по отношению к категории информация механизм её использования, отвечая на вопрос «как?». То есть, ставится вопрос не о защите данных и информации, а о защите знаний как категории более ценной, требования по защите которых должны быть на порядок выше требований по защите информации. В этой связи возникает еще и дополнительный аспект информационной безопасности – появление псевдознаний, псевдонаук, которые в больших объемах может генерировать искусственный интеллект. Это требует рассмотрения второго из двух базовых аспектов информационной безопасности – защита человека и общества от воздействия на них ложной и деструктивной информации, псевдознаний и псевдонаук, что становится всё более очевидным в настоящее время, по мере углубления вхождения ведущих мировых держав в информационное общество, индикатором чего является необратимое развитие цифровой экономики.

Ключевые слова: данные, информация, знания, мудрость, концепция DIKW, псевдознания, псевдонауки, искусственный интеллект, информационная безопасность, гуманитарные аспекты информационной безопасности, чат-боты, чат-бот ChatGPT, Yandex GPT.

KNOWLEDGE SECURITY WHEN USING GPT CHATBOTS

P.Yu. Filyak, A.N. Dymov, K,P,Kolpakov

Information security in the era of Industry 4.0 is considered through the prism of Russell Akoff's concept – the famous DIKW pyramid, in which knowledge, as is known, is one of the strata of this pyramid, standing above information and adding a mechanism for its use in relation to the information category, answering the question "how?". The question is not about data protection, but about knowledge protection, since knowledge is a more valuable category and therefore the requirements for knowledge protection should be an order of magnitude higher than when protecting information. In this regard, there is also an additional aspect of information security – the emergence of pseudoscience, pseudoscience, which artificial intelligence can generate in large volumes. This requires consideration of the second of the two basic aspects of information security – the protection of man and society from the impact on them of false and destructive information, pseudoscience and pseudoscience.

Keywords: data, information, knowledge, wisdom, DIKW concept, pseudoscience, pseudoscience, artificial intelligence, information security, humanitarian aspects of information security, chatbots, chatbots ChatGPT, Yandex GPT.

DOI 10.36622/VSTU.2023.26.3.026
УДК 004.942:004.056

ФАКТОРЫ И СПОСОБЫ ВЛИЯНИЯ НА РАСПРОСТРАНЕНИЕ ФЕЙКОВ В СОЦИАЛЬНЫХ СЕТЯХ

А.А. Караханова, В.И. Белоножкин

Социальные сети и новостные агентства все чаще публикуют фальшивые (фейковые) новости для увеличения читательской аудитории или в рамках информационной войны, поэтому проблема обнаружения фейков в социальных сетях становится все более актуальной. В статье рассмотрено влияние вредоносных и интеллектуальных узлов на распространение ложной информации с применением модели простого заражения сети. Исследована динамика перехода узлов в различные состояния – восприимчивое, принимающее и иммунизированное.Предложено решение, которое можно использовать для снижения вероятности распространения фейков на примере обнаружения и фильтрации кликбейтов, эффективность которого была подтверждена экспериментально.

Ключевые слова: ложная информация, фейк, социальная сеть, кликбейт, моделирование.

MEANS AND METHODS OF MONITORING AND PREVENTION OF THE DISTRIBUTION OF FALSE INFORMATION

A.A. Karakhanova, V.I. Belonozhkin

Social networks and news agencies are increasingly publishing fake news to increase readership or as part of psychological warfare, so the problem of detecting fakes in social networks is only gaining relevance. The article considers the impact of malicious nodes on the spread of false information using a simple infection model with the inclusion of intelligent nodes that recognize false information better than ordinary nodes. The dynamics of the transition of nodes to various states - susceptible, receiving and immunized - was investigated. A solution has been proposed that can be used to reduce the likelihood of the spread of fakes using the example of detecting and filtering clickbates, the effectiveness of which has been confirmed experimentally.

Keywords: false information, fake, social network, clickbait,

DOI 10.36622/VSTU.2023.26.3.013
УДК 004.056.57

ПОЛИГОННЫЕ КИБЕРУЧЕНИЯ НА ПРИМЕРЕ МОДЕЛИРОВАНИЯ КОМПЬЮТЕРНЫХ ЭПИДЕМИЙ СЕТЕЙ

Е.А. Москалева, А.И. Шеншин, И.А. Каданцев

В настоящее время повсеместное применение киберполигонов продолжает набирать обороты, расширяя возможности и повышая эффективность информационной защиты систем. Количество и качество преднамеренных информационных угроз, неуклонно растет, включая атаки с применением вредоносного программного обеспечения. Значительную угрозу представляют вредоносы, способные порождать масштабные сетевые эпидемии, поскольку их деструктивное воздействие позволяет быстро и эффективно наносить значительный финансовый и репутационный ущерб организациям и частным лицам. Несмотря на значительный прогресс в исследовании в области сетевой эпидемиологии, актуальным остается вопрос эффективной оценки и регулирования рисков возникновения компьютерных эпидемий в сетях. В статье обсуждается методика моделирования эпидемии сети, учитывающая диффузию вирусного программного обеспечения. Рассматриваемая методика предусматривает программную реализацию моделирования процессов размножения и диффузии вирусного программного обеспечения в атакуемой телекоммуникационной сети. На основе методики проводились киберучения на базе киберполигона кафедры систем информационной безопасности Воронежского государственного университета.

Ключевые слова: киберполигон, эпидемический процесс, компьютерная эпидемия, вредоносное программное обеспечение, дискретное моделирование, информационная безопасность.

POLYGON CYBER EXERCISES ON THE EXAMPLE OF SIMULATION OF COMPUTER EPIDEMICS OF NETWORKS

E.A. Moskaleva, A.I. Shenshin, A.A. Ostapenko, I.A. Kadantsev

Currently, the widespread use of cyber ranges continues to gain momentum, expanding the capabilities and increasing the efficiency of information protection of systems. The number and quality of deliberate information threats is steadily growing, including attacks using malicious software. Malware that can cause large-scale network epidemics poses a significant threat, since their destructive effects can quickly and effectively cause significant financial and reputational damage to organizations and individuals. Despite significant progress in research in the field of network epidemiology, the issue of effective assessment and regulation of the risks of computer epidemics in networks remains relevant. The article discusses a technique for modeling a network epidemic that takes into account the diffusion of virus software. The technique under consideration involves a software implementation of modeling the processes of reproduction and diffusion of viral software in an attacked telecommunications network. Based on the methodology, cyber exercises were conducted at the cyber training ground of the Department of Information Security Systems of Voronezh State University.

Keywords: cyber training ground, cyber testing ground, epidemic process, computer epidemic, malicious software, discrete modeling, information security.

DOI 10.36622/VSTU.2023.26.3.014
УДК 004.056

ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ: НАУЧНО-МЕТОДИЧЕСКОЕ РАЗВИТИЕ В НАПРАВЛЕНИИ ВНЕДРЕНИЯ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ОРГАНИЗАЦИОННО-ПРАВОВОЙ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ

А.Г. Остапенко, Д.В. Щербакова, А.А. Остапенко, Д.А. Нархов

Рассматривается целеполагание проектной деятельности, реализуемой на основе искусственных нейросетей. Описываются задачи и модули подобной реализации, её нормативного обеспечения. Для создания информационного обеспечения нейросети предлагаются таблицы, формирующие базу знаний по организационно-правовому обеспечению (частные политики, регламенты и инструкции безопасности) защиты корпоративных сетей. Также вниманию студентов предлагаются варианты заданий для широкого многообразия компьютерных атак, для которых требуется разрабатывать необходимые политики, регламенты и инструкции. В случае регистрации одной из них, нейросеть выдает администратору корпоративной сети интеллектуальную подсказку по эффективному противодействию вторжению. Машинное обучение нейросети будет повышать точность её решений по мере эксплуатации средств искусственного интеллекта.

Ключевые слова: искусственный интеллект, безопасность, атаки, организационно-правовая защита, проектная деятельность.

PROJECT ACTIVITIES: SCIENTIFIC AND METHODOLOGICAL DEVELOPMENT IN THE DIRECTION OF THE INTRODUCTION OF ARTIFICIAL INTELLIGENCE TOOLS TO ENSURE ORGANIZATIONAL AND LEGAL PROTECTION OF CORPORATE NETWORKS

A.G. Ostapenko, D.V. Shcherbakova, A.A. Ostapenko, D.A. Narhov

The goal-setting of project activities implemented on the basis of artificial neural networks is considered. The tasks and modules of such implementation, its normative support are described. To create information support for neural networks, tables are proposed that form a knowledge base on organizational and legal support (private policies, regulations and security instructions) for the protection of corporate networks. Also, students are offered options for tasks for a wide variety of computer attacks, for which it is required to develop the necessary policies, regulations and instructions. In case of registration of one of them, the neural network gives the administrator of the corporate network an intelligent hint on effective counteraction to intrusion. Machine learning of a neural network will increase the accuracy of its decisions as artificial intelligence tools are used.

Keywords: artificial intelligence, security, attacks, organizational and legal protection, project activity.