DOI 10.36622/VSTU.2023.26.1.001
УДК 004.056

КИБЕРПОЛИГОН КАК ПРОЕКТ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Г.А. Остапенко, В.И. Белоножкин, А.А. Остапенко, М.Е. Волкова

В работе рассматривается проект создания киберполигона в качестве тренажера тестируемых систем на предмет управления рисками успешности реализации сетевых атак. В этой связи обсуждаются принципы оценки и регулирования рисков от университетской подготовки специалистов до их тренингов условиях создаваемого полигона. Предлагается соответствующий глоссарий и рассматриваются предпосылки для полигонной организации. При этом, киберсистема определяется как социо-техническая сущность, в которой полигоном эмулируется процесс информационного противоборства. В этой связи, формулируются задачи построения киберполигона, оценивается их инновационность. Впервые описываются области возможного сотрудничества университета и IT-предприятий в вопросах построения киберполигона, а также – мотивы инновационной интеграции участников проекта.

Ключевые слова: киберсистема, киберполигон, информационные риски, эмуляция, инновация.

CYBERPOLYGON AS A PROJECT OF INFORMATION RISK MANAGEMENT

G.A. Ostapenko, V.I. Belonozhkin, A.A. Ostapenko, M.E. Volkova

The paper considers the project of creating a cyberpolygon as a simulator of tested systems for managing the risks of successful implementation of network attacks. In this regard, the principles of risk assessment and management are discussed from the university training of specialists to their training under the conditions of the created test site. A related glossary is proposed and prerequisites for a landfill organization are considered. At the same time, the cyber system is defined as a socio-technical entity in which the process of information confrontation is emulated by a testing ground. In this regard, the tasks of building a cyberpolygon are formulated, their innovativeness is assessed. For the first time, the areas of possible cooperation between the university and IT enterprises in the construction of a cyberpolygon are described, as well as the motives for the innovative integration of project participants.

Keywords: cybersystem, cyberpolygon, information risks, emulation, innovation.

DOI 10.36622/VSTU.2023.26.1.002
УДК 004.735

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ПРИ АТАКАХ, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ ПРОТОКОЛОВ ПРИКЛАДНОГО УРОВНЯ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.А. Котышенко, А.А. Болгов, Ю.Г. Пастернак, А.Г. Краснобородкин

Предложено методическое обеспечение количественной оценки рисков, а также алгоритмическое обеспечение регулирования рисков нарушения конфиденциальности информации при атаках, использующих уязвимости протоколов прикладного уровня в телекоммуникационных системах Интернета вещей. Разработана модель системы, учитывающая архитектуру и топологию телекоммуникационной системы «умный дом», а также модель угроз, включающая в себя набор уязвимостей и атак для каждого устройства и описание возможностей злоумышленника. Алгоритмическое обеспечение регулирования рисков основано на модели системы «умный дом», построенной по полносвязной топологии, и предназначено для выявления в ней наиболее уязвимых компонентов и формирования набора мер для увеличения защищенности. Полученные результаты в виде численной оценки и алгоритмического обеспечения позволяют адекватно оценить состояние защищенности телекоммуникационной системы «умный дом» и сформировать набор мер по её повышению.

Ключевые слова: умный дом, риск, конфиденциальность, телекоммуникационная система, полносвязная топология.

ASSESSMENT AND REGULATION OF RISKS OF VIOLATION OF CONFIDENTIALITY OF INFORMATION IN ATTACKS USING VULNERABILITIES OF APPLICATION LAYER PROTOCOLS IN TELECOMMUNICATION SYSTEMS OF THE INTERNET OF THINGS

S.A. Ermakov, A.A. Kotyshenko, A.A. Bolgov, Yu.G. Pasternak, A.G. Krasnoborodkin

A methodical tooling for quantitative risk assessment is proposed, as well as algorithmic tooling for regulating the risks of information confidentiality violation during attacks that use vulnerabilities in application-level protocols in telecommunication systems of the Internet of things. A system model has been developed that takes into account the architecture and topology of the "smart home" telecommunications system, as well as a threat model that includes a set of vulnerabilities and attacks for each device and a description of the attacker's capabilities. Algorithmic provision of risk management is based on the model of the "smart home" system, built on a full-mesh topology, and is intended to identify the most vulnerable components in it and form a set of measures to increase security. The obtained results in the form of a numerical assessment and algorithmic support make it possible to adequately assess the state of security of the "smart home" telecommunication system and form a set of measures to improve the security of the system.

Key words: smart home, risk, privacy, telecommunication system, full-mesh topology.

DOI 10.36622/VSTU.2023.26.1.003
УДК 519.766.4:004.032.26

«ПРОСЕИВАНИЕ» ТЕЛЕГРАМ-КАНАЛОВ ПРИ ПОИСКЕ КОНТЕНТА ЭКСТРЕМИСТСКОГО ХАРАКТЕРА

В.А. Минаев, А.В. Симонов

Предложено решение задачи поиска и обнаружения каналов экстремистской направленности в наиболее популярном мессенджере Telegram. Разработан метод, основанный на использовании глубоких искусственных нейронных сетей BERT в качестве классификатора текстов. На его основе разработана программа, позволяющая в автоматизированном режиме осуществлять анализ телеграмм-каналов и выявлять материалы экстремистского характера. Описаны пять этапов разработки программы «просеивания» каналов: формирование текстовых корпусов для обучения BERT; выбор архитектуры BERT и обучение классификатора; выгрузка сообщений из анализируемых каналов; оценка наличия экстремизма в сообщениях; оценка каналов на экстремизм. Для апробации метода и программного продукта проведена серия экспериментов, в ходе которых осуществлен мониторинг 68 каналов по 8 категориям с целью их «просеивания» на наличие экстремистского контента. По результатам экспериментов ранжированы телеграмм-каналы, распространяющие экстремистские материалы. Оценена доля сообщений экстремистского характера в каждой категории каналов. Сделан вывод, что представленный подход к «просеиванию» телеграмм-каналов на наличие экстремистских сообщений целесообразно использовать в работе государственных структур, занимающихся выявлением и мониторингом распространения противоправной информации.

Ключевые слова: мессенджер Telegram, деструктивный контент, нейронная сеть, экстремизм, трансформер BERT.

SCREENING OF TELEGRAM CHANNELS WHEN SEARCHING FOR EXTREMISM CONTENT

V.A. Minaev, A.V. Simonov

A solution to the problem of searching and detecting extremist channels in the most popular Telegram messenger is proposed. A method based on the use of deep artificial neural networks BERT as a classifier of texts has been developed. Based on it, a program has been developed that allows automated analysis of telegram channels and identification of extremist materials. Five stages of the development of the channel "sifting" program are described: the formation of text corpora for BERT training; the choice of the BERT architecture and the training of the classifier; unloading messages from analyzed channels; assessing the presence of extremism in messages; evaluating channels for extremism. To test the method and the software product, a series of experiments were conducted, during which 68 channels were monitored in 8 categories in order to "sift" them for the presence of extremist content. According to the results of the experiments, telegram channels disseminating extremist materials were ranked. The share of extremist messages in each category of channels is estimated. It is concluded that the presented approach to "sifting" telegram channels for the presence of extremist messages is advisable to use in the work of state structures engaged in identifying and monitoring the dissemination of illegal information.

Keywords: Telegram messenger, destructive content, extremism, neural network, transformer BERT.

DOI 10.36622/VSTU.2023.26.1.004
УДК 004.732

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ НАРУШЕНИЯ ДОСТУПНОСТИ ИНФОРМАЦИИ ПРИ РЕАЛИЗАЦИИ АТАК НА СЕТИ ИНТЕРНЕТА ВЕЩЕЙ, ПОСТРОЕННЫЕ НА БАЗЕ ТЕХНОЛОГИИ SDN

С.А. Ермаков, И.И. Донсков, А.А. Болгов, О.Ю. Макаров, Р.Д. Бурцев

В данной статье предлагается методическое и алгоритмическое обеспечение количественной оценки рисков нарушения доступности систем Интернета вещей, построенных на базе программно-определяемых сетей (SDN). Предлагаемое обеспечение учитывает особенности построения выбранных сетей. Потенциальный ущерб складывается как из ценности защищаемых активов, так и из особенностей топологии рассматриваемой сети. Вероятность атаки определяется индивидуально для каждого типа злоумышленников, с учетом его ресурсов и мотивации. Представлена методика регулирования риска, представляющая собой механизм двойной маршрутизации с учётом рисков, основанный на эволюционном алгоритме. Предложенный алгоритм позволяет вычислить наиболее оптимальные настройки системы, обеспечивая при этом приемлемое время сходимости. Обширные результаты моделирования предложенного подхода демонстрируют повышение защищенности различных сетевых топологий без значительного ущерба производительности.

Ключевые слова: Интернет вещей, программно-определяемая сеть (SDN), риск, доступность, маршрутизация.

ASSESSMENT AND RISK MENAGEMENT OF INFORMATION AVAILABILITY OF SDN-BASED INTERNET OF THINGS NETWORKS

S.A. Ermakov, I.I. Donskov, A.A. Bolgov, O.Yu. Makarov, R.D. Burtsev

This article proposes methodology and algorithm for quantifying risks assessment of availability breaches of SDN-based Internet of things systems. The proposed methodology considers the features of selected networks structure. Potential damage consists both of the protected assets worth and the topology specificity. The probability of an attack is determined individually for each attacker type, taking into account his resources and motivation. A risk management methodology is proposed. It represents a risk-aware dual routing mechanism, based on evolutional algorithm. Proposed algorithm makes it possible to calculate the most optimal system settings, while providing an acceptable convergence time Extensive simulation results demonstrate an increase in security level in various network topologies without essential performance reducing.

Keywords: Internet of Things, software-defined network (SDN), risk, availability, routing.

DOI 10.36622/VSTU.2023.26.1.005
УДК 004.046

ИНСТРУМЕНТАРИЙ АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ НАРУШЕНИЯ КОНФЕДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ РАЗМЕЩЕНИИ В ОТЕЧЕСТВЕННЫХ ХРАНИЛИЩАХ

И.А. Моисеев, Л.В. Паринова, Д.А. Нархов

Данная статья посвящена защите скомпрометированных персональных данных пользователей, находящихся в публичном доступе, а также оценке и регулированию рисков нарушения конфиденциальности данных при их размещениях в открытых хранилищах. В основе методики лежит алгоритм защиты и регулирования личных данных пользователя в информационно телекоммуникационной сети «Интернет». В работе представлены способы защиты конфиденциальной информации и методы борьбы с ресурсами, направленными на сбор и неправомерное использование персональной информации, подверженной компрометации со стороны злоумышленника.

Ключевые слова: персональные данные, риск, конфиденциальность, утечки, база данных.

TOOLS FOR AUTOMATED ASSESSMENT AND REGULATION OF RISKS OF VIOLATION OF THE CONFIDENTIALITY OF PERSONAL DATA WHEN THEY ARE PLACED IN DOMESTIC REPOSITORIES

I.A. Moiseev, L.V. Parinova, D.A. Narkhov

This article is devoted to the protection of compromised personal data of users in the public domain, as well as the assessment and regulation of the risks of data privacy violations when they are placed in open repositories. The methodology is based on an algorithm for protecting and regulating the user's personal data in the Internet information and telecommunications network. The paper presents ways to protect confidential information and methods of combating resources aimed at collecting and misuse of personal information subject to compromise by an attacker.

Keywords: personal data, risk, confidentiality, leaks, database.

DOI 10.36622/VSTU.2023.26.1.006
УДК 004.35:004.732

ВЕЙВЛЕТ-ТЕХНОЛОГИИ ДЛЯ ШУМООЧИСТКИ РЕЧЕВЫХ СИГНАЛОВ В ОПТИКО-ЭЛЕКТРОННЫХ КАНАЛАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

А.В. Бабурин, Л.А. Глущенко, А.М. Корзун

Шумоочистка играет важную роль при оценке эффективности защиты объектов от несанкционированного доступа к речевой информации по оптико-электронным каналам. В работе оценивается эффективность использования шумоочистки речевых сигналов на основе применения вейвлет-анализа. Качество речевой информации, полученной по оптико-электронным каналам несанкционированного доступа, как правило, очень низкое, поэтому вопросы шумоочистки для этих каналов весьма актуальны. Приведено описание таких каналов. Экспериментальная проверка возможности применения вейвлет-анализа для шумоочистки речевых сигналов проведена с помощью лабораторной установки, которая предназначена для физического моделирования аппаратуры регистрации лазерного излучения, отраженного от поверхности, вибрирующей под воздействием речевого акустического сигнала. Показано, что применение вейвлет-анализа для шумоочистки сигналов позволяет существенно повысить эффективность оптико-электронных каналов несанкционированного доступа к речевой информации.

Ключевые слова: оптико-электронный канал, несанкционированный доступ, речевая информация, вейвлет-анализ, словесная разборчивость речи.

THE USE OF WAVELET TECHNOLOGIES FOR NOISE CLEANING OF SIGNALS IN OPTICAL-ELECTRONIC CHANNELS OF UNAUTHORIZED ACCESS TO SPEECH INFORMATION

A.V. Baburin, L.A. Glushchenko, A.M. Korzun

Noise cleaning plaes an importent role in assessing the effectiveness of protecting objects from unauthorized access to speech information. The paper considers the possibility of using noise cleaning of speech signals based on the use of wavelet analysis. The quality of speech information received by optical-electronic channels of unauthorized access is usually very low. Noise reduction issues for these channels are very relevant. The discription of such channels is given. An experimental verification of the possibility of using wavelet analysis for noise cleaning of speech signals was carriad out using a laboratory setap designed for physical modeling of of equipment for recording laser radiation reflected from the surface vibrating under the influence of a speech acoustic signal. It is shown that the use of wavelet analysis for nose cleaning of signals can significantly increase the efficiency of channels for optoelectronic channels of unauthorized access to speech information.

Keyword: optical-electronic channel, unauthorized access, speech information, wavelet analysis, verbal intelligibility.

DOI 10.36622/VSTU.2023.26.1.007
УДК 004.733

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ РЕАЛИЗАЦИИ АТАКИ «SINKHOLE» НА БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ, СОСТОЯЩИЕ ИЗ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, Ю.А. Ермаченко, А.А. Болгов, В.Н. Кострова, А.А. Сиделев

В данной статье предлагаются методики количественной оценки и регулирования рисков успешной реализации атаки «Sinkhole», направленной на нарушение конфиденциальности, целостности и доступности данных и влияющей на жизненно важные для сетей Интернета вещей показатели – энергоэффективность и пропускную способность устройства на этапе проектирования системы. Данная методика основана на применении четырехслойной риск модели, как оптимальном способе оценки риска. Разработаны алгоритмы для количественной оценки риска и регулирования рисков на этапе начала эксплуатации системы. Они основаны на получении информации об уязвимостях из публичных источников – реестров уязвимостей, экспертных оценок. Представлен программный инструментарий, для сравнения конфигурации сети, который позволяет выбирать и сравнивать различные наборы мер и средств защиты сети и устройств в соответствии с предложенными методиками и алгоритмами оценки и регулирования рисков, как итог, выбрать наиболее оптимальную относительно риска и используемых материальных ресурсов для использования конфигурацию с точки зрения риска успешной реализации атаки «Sinkhole».

Ключевые слова: Интернет вещей, беспроводная сенсорная сеть, риск, экспертные оценки, четырехслойная риск модель, энергоэффективность, защищенность.

ASSESSMENT AND REGULATION OF THE RISKS OF IMPLEMENTING «SINKHOLE» ATTACKS ON WIRELESS SENSOR NETWORKS CONSISTING OF INTERNET OF THINGS DEVICES

S.A. Ermakov, Y.A. Ermachenko, A.A. Bolgov, V.N. Kostrova, A.A. Sidelev

This article proposes methods for quantifying and managing the risks of a successful «Sinkhole» attack aimed at violating confidentiality, integrity and availability of data and affecting vital indicators for the Internet of Things networks – energy efficiency and device throughput at the system design stage. This technique is based on the use of a four-layer risk model as the optimal way to assess risk. Algorithms have been developed for quantitative risk assessment and risk management at the start-up stage of the system. They are based on obtaining information about vulnerabilities from public sources – vulnerability registries, expert assessments. A software toolkit is presented to select the optimal network configuration, which allows you to select and compare different sets of measures and means of protecting the network and devices in accordance with the proposed methods and algorithms for risk assessment and management, as a result, to choose the most optimal configuration for use in terms of the risk of successful implementation of the «Sinkhole» attack.

Keywords: Internet of things, wireless sensor network, risk, expert assessments, four-layer risk model, energy efficiency, security.

DOI 10.36622/VSTU.2023.26.1.008
УДК 004.735

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ПОСТРОЕННЫХ НА БАЗЕ ПРОТОКОЛА BGP: АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ РЕАЛИЗАЦИИ АТАКИ IP-HIJACKING

К.А. Разинкин, А.А. Науменко, А.И. Мордовин, О.Н. Чопоров, Ю.В. Макаров

В статье предложена методика повышения защищенности телекоммуникационных сетей, построенных на базе протокола BGP от атаки IP-hijacking, направленной на нарушение конфиденциальности и доступности перехваченной информации автономных систем. Ключевой составляющей данной методики является алгоритм оценки и регулирования рисков успешной реализации атаки IP-hijacking на телекоммуникационную сеть. В работе представлены особенности топологии телекоммуникационной сети, построенной на базе протокола BGP, и специфика атаки IP-hijacking, типовой сценарий реализации атаки, включающий описание уязвимостей сетевого оборудования, структура векторов и математическая оценка потенциала атаки IP-hijacking, также предложен инструментарий оценки и регулирования рисков. Полученные результаты в виде графика уровней риска позволяют определять область и возможные средства регулирования рисков сети, а также рассматривать возможный уровень ущерба конфиденциальности и доступности информации автономных систем.

Ключевые слова: протокол BGP, риск, атака IP-hijacking, конфиденциальность, телекоммуникационная сеть.

IMPROVING THE SECURITY OF TELECOMMUNICATION NETWORKS BUILT ON THE BASIS OF THE BGP PROTOCOL: ALGORITHMIC SUPPORT FOR THE ASSESSMENT AND REGULATION OF IMPLEMENTATION RISKS IP HIJACKING ATTACKS

K.A. Razinkin, A. A. Naumenko, A.I. Mordovin, O.N. Choporov, Yu.V. Makarov

The article proposes a method for improving the security of telecommunication networks built on the basis of the BGP protocol from an IP-hijacking attack aimed at violating the confidentiality and availability of intercepted information of autonomous systems. A key component of this methodology is an algorithm for assessing and managing the risks of a successful IP-hijacking attack on a telecommunications network. The article presents the features of the topology of a telecommunications network built on the basis of the BGP protocol and the specifics of the IP-hijacking attack, a typical scenario for the implementation of an attack, including a description of network equipment vulnerabilities, the structure of vectors and a mathematical assessment of the potential of an IP-hijacking attack, as well as a toolkit for risk assessment and management. The results obtained in a graph of risk levels make it possible to determine the scope and possible means of regulating network risks, as well as to consider the possible level of damage to the confidentiality and availability of information of autonomous systems.

Key words: BGP protocol, risk, IP-hijacking attacks, privacy, telecommunication network.

DOI 10.36622/VSTU.2023.26.1.009
УДК 004.732

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ РЕАЛИЗАЦИИ АТАК, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ ПРИКЛАДНОГО И СЕТЕВОГО УРОВНЕЙ, НА СЕНСОРНЫЕ УСТРОЙСТВА ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, Д.Р. Серых, А.А. Болгов, И.Л. Батаронов, А.С. Кривошеин

В статье предлагается методика оценки и регулирования рисков для повышения защищенности сенсорных устройств промышленного Интернета вещей от атак, использующих уязвимости прикладного и сетевого уровней, направленных на нарушение конфиденциальности, целостности и доступности информации. Методика позволяет проводить оценку риска с учетом основных технических характеристик программных, аппаратных и прошивочных уязвимостей. Процесс регулирования риска включает в себя переоценку риска реализации атаки на конкретное устройство с учётом использования мер противодействия. Представлен программный инструментарий, для оценки и регулирования рисков, позволяющий сравнивать значения риска при использовании различных мер противодействия ему. Полученные результаты в виде количественной оценки позволяют провести анализ рисков реализации возможных атак на каждое из устройств сети, выявлять наиболее уязвимые элементы сети, а также подобрать меры для снижения уровня риска до необходимого значения.

Ключевые слова: промышленный Интернет вещей, риск, атака, конфиденциальность, целостность, доступность.

ASSESSMENT AND REGULATION OF THE RISKS OF ATTACKS USING VULNERABILITIES OF THE APPLIED AND NETWORK LEVEL ON SENSOR DEVICES OF THE INDUSTRIAL INTERNET OF THINGS

S.A. Ermakov, D.R. Seryh, A.A. Bolgov, I.L. Bataronov, A.S. Krivoshein

The article proposes a methodology for assessing and managing risks to increase the security of industrial Internet of Things sensor devices from attacks that use vulnerabilities in the application and network layers aimed at violating the confidentiality, integrity and availability of information. The technique allows to carry out a risk assessment taking into account the main technical characteristics of software, hardware and firmware vulnerabilities. The risk management process involves reassessing the risk of an attack on a particular device, taking into account the use of countermeasures. A software toolkit is presented for assessing and managing risks, which makes it possible to compare risk values when using various measures to counteract it. The obtained results in the form of a quantitative assessment make it possible to analyze the risks of implementing possible attacks on each of the network devices, identify the most vulnerable elements of the network, and select measures to reduce the risk level to the required value.

Keywords: Industrial Internet of Things, risk, attack, confidentiality, integrity, availability.

DOI 10.36622/VSTU.2023.26.1.010
УДК 004.735

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫХ НА БАЗЕ ТЕХНОЛОГИЙ NFV/SDN: МЕТОДИКА И АЛГОРИТМ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Н.И. Баранников, Н.Н. Мурзинов, В.Г. Юрасов, В.Ю. Остапенко

В статье рассмотрена методика повышения защищенности телекоммуникационных систем, построенных на базе технологий NFV/SDN, от атак, направленных на нарушение конфиденциальности информации. В основе методики лежит алгоритм численной оценки и регулирования рисков для каждого компонента NFV/SDN системы с учетом их специфики и возможностей злоумышленников.

Ключевые слова: NFV/SDN, риск, атака, конфиденциальность, виртуализация.

IMPROVING THE SECURITY OF TELECOMMUNICATION SYSTEMS BASED ON NFV/SDN TECHNOLOGIES: METHODOLOGY AND ALGORITHM FOR ASSESSING THE RISKS OF INFORMATION PRIVACY VIOLATIONS

N.I. Barannikov, N. N. Murzinov, V.G. Yurasov, V.Yu. Ostapenko

The article discusses a technique for improving the security of telecommunication systems built on the basis of NFV/SDN technologies from attacks aimed at violating the confidentiality of information. The methodology is based on an algorithm for numerical assessment and risk management for each component of the NFV/SDN system, taking into account their specifics and the capabilities of intruders.

Key words: NFV/SDN, risk, attack, privacy, virtualization.

DOI 10.36622/VSTU.2023.26.1.011
УДК 004.056.5

СОЗДАНИЕ «КИБЕРПОЛИГОНА»: РЕАЛИЗАЦИЯ ИНФОРМАЦИОННОГО КАРТОГРАФИРОВАНИЯ РИСКОВ, СВЯЗАННЫХ С ПУБЛИКАЦИЕЙ СВЕДЕНИЙ ОБ УЯЗВИМОСТЯХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А.Л. Сердечный, М.А. Булычев, А.А. Гончаров, М.И. Ярмонов, А.Ю. Егоров

Статья посвящена вопросам создания модуля информационного картографирования рисков, связанных с публикацией сведений об уязвимостях программного обеспечения в рамках проекта «Киберполигон». Потребность в данном проекте обусловлена необходимостью тренировки навыков противодействия как специалистов в сфере информационной безопасности, так и студентов данной предметной области. Наглядное представление различных классов уязвимостей, и связанных с ними рисков реализации угроз безопасности информации, позволяет проводить своевременный процесс приоритезации, аналитики и снижения ущерба информационным системам. Целью создания данного модуля является повышение качества и результативности учебного процесса при исследовании атак на информационные системы за счет применения метода информационного картографирования к источникам, содержащим сведения об уязвимостях программного обеспечения. Для этой цели был разработан облик блока информационного картографирования рисков с интегрированными модулями тренинга в сфере информационного противоборства, который представляется вниманию научной общественности.

Ключевые слова: информационная картография, киберполигон, платформа картографирования рисков, анализ, визуализация.

CREATION OF A "CYBERPOLYGON": IMPLEMENTATION OF INFORMATION MAPPING OF RISKS ASSOCIATED WITH THE PUBLICATION OF INFORMATION ABOUT SOFTWARE VULNERABILITIES

A.L. Serdecniy, M.A. Bulychev, A.A. Goncharov, M.I. Yarmonov, A.Yu. Egorov

The article is devoted to the issues of creating an information mapping module for risks associated with the publication of information about software vulnerabilities within the framework of the Cyberpolygon project. The need for this project is due to the need to train counteraction skills of both specialists in the field of information security and students of this subject area. A visual representation of various classes of vulnerabilities, and the associated risks of information security threats, allows for a timely process of prioritization, analytics and damage reduction to information systems. The purpose of creating this module is to improve the quality and effectiveness of the educational process in the study of attacks on information systems by applying the method of information mapping to sources containing information about software vulnerabilities. For this purpose, the image of the risk information mapping unit with integrated training modules in the field of information warfare was developed, which is presented to the attention of the scientific community.

Keywords: information cartography, cyberpolygon, risk mapping platform, analysis, visualization.

DOI 10.36622/VSTU.2023.26.1.012
УДК 004.056

РАЗРАБОТКА АРХИТЕКТУРЫ КИБЕРПОЛИГОНА ДЛЯ ПОВЫШЕНИЯ КАЧЕСТВА И РЕЗУЛЬТАТИВНОСТИ УЧЕБНОГО ПРОЦЕССА В ИССЛЕДОВАНИИ АТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ И СЕТИ

Г.А. Остапенко, С.С. Куликов, А.В. Коноплин, А.А. Остапенко

В статье предложен подход к созданию «Киберполигона». В основе подхода лежит разбиение архитектуры на блоки. Такой подход представляет возможность развития и масштабирования системы в перспективе. Модульная архитектура обеспечит фундамент для развития предлагаемого решения и позволит модифицировать с учетом специфических тонкостей информационных сетей. В работе представлены схемы функционирования различных блоков общей архитектуры, учитывающие полное обеспечение пользователя полигона необходимой информацией и проверкой различных аспектов тестируемой сети. Предложенные в работе модули могут стать основой для обобщенной системы, которая позволит пользователю услугу по полноценному анализу выбранной информационной системы. Представленные результаты основаны на опыте уже созданных решений, с учетом их недостатков и преимуществ. Целью разработки архитектуры является повышение качества и результативности учебного процесса в исследовании атак на информационные системы и сети.

Ключевые слова: киберпространство, киберполигон, сеть, атака.

DEVELOPMENT OF A CYBER POLYGON ARCHITECTURE TO IMPROVE THE QUALITY AND EFFECTIVENESS OF THE TRAINING PROCESS IN THE STUDY OF ATTACKS ON INFORMATION SYSTEMS AND NETWORKS

G.A. Ostapenko, S. S. Kulikov, A.V. Konoplin, A.A. Ostapenko

The article proposes an approach to creating a Cyberpolygon. The approach is based on the partitioning of the architecture into blocks. This approach presents an opportunity to develop and scale the system in the future. The modular architecture will provide a foundation for the development of the proposed solution and allow modification to take into account the specific subtleties of information networks. In the work schemes of functioning of different blocks of general architecture, taking into account full maintenance of the polygon user with necessary information and verification of different aspects of tested network are presented. The modules proposed in the work can become the basis for a generalized system that will allow the user to fully analyze the selected information system. The presented results are based on the experience of already created solutions, taking into account their disadvantages and advantages. The purpose of developing the architecture is to improve the quality and effectiveness of the learning process in the study of attacks on information systems and networks.

Keywords: cyberspace, cyber training ground, network, attack.