АННОТАЦИЯ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время существует необходимость в автоматизации рутинных процессов. Более 70 лет мировой истории это представлялось людям, как прислуживающие роботы, но теперь эти процессы стали более известны как IoT. Эта сфера помогает автоматизировать повторяющиеся задачи, проконтролировать протекание длительных процессов, уменьшить потребление ресурсов, таких как электроэнергия, и др.

В ряде западных стран такие системы интегрированы на многие предприятия, заводы, или просто вплетены в городскую среду, например, для контроля освещенности улиц. В Российской Федерации данная сфера находится на этапе активного внедрения у частных компаний, которые используют IoT для современных технологических производств, экономя средства на излишней работе станков. Внедрение IoT в Российской Федерации на данный момент не является достаточным, что делает актуальной тему данного исследования.

Целью НИР является анализ зарубежных и отечественных источников для формирования представления о веб-технологиях, используемых в сфере IoT.

Объектом исследования являются информационные системы, осуществляющие управления элементами IoT.

Предметом исследования являются результаты анализа отечественной и зарубежной литературы по теме исследования.

Задачи исследования:

- Составить обзор российских и зарубежных научных исследований, посвященных IoT.
- Провести анализ отечественных научных исследований о существующих разработках в сфере IoT.
- Провести анализ зарубежных научных исследований в области проектирования IoT сервисов.

Теоретические основы исследования. При анализе источников было выявлено, что тема внедрения элементов IoT освещена подробно, однако массового внедрения этой технологии на территории Российской Федерации не было.

В работе (Г.Ю. Портянкин, О.Ю. Рязанов) описаны принципы работы новой системы, которая позволяет решать ряд расчетных задач сельского хозяйства, получая и обрабатывая данные с умных устройств. По исследованию (Н.В. Рогачева) автор подытоживает текущие проблемы сферы и задачи, которые необходимо решить, чтобы продвинуть эту сферу вперед в Российской Федерации.

В трудах зарубежных авторов (M. Stusek, K. Zeman, P. Masek, J. Hosek, J. Sedova) подробно рассмотрены IOT протоколы передачи данных и перспективы их развития.

В рассмотренных источниках были приведены примеры реализации системы на IoT устройствах, однако сегодня сервисы, по которым были приведены примеры, не существуют по причине закрытия или нерелевантного принципа работы. Приведенные факторы обуславливают **актуальность темы научно-исследовательской работы**.

Информационная база исследования: eLIBRARY, CyberLeninka ResearchGate.

Методы исследования. Для решения задач исследования использовался комплекс теоретических и эмпирических взаимодополняющих методов исследования, среди которых ведущими были следующие методы: анализ, сравнение и обобщение, методы индукции и дедукции.

Результаты исследования. Проведенный анализ: ˜ ведущих трендов социально-экономического и технологического развития показал, что проблема освещенности сферы интернета вещей в Российской Федерации является актуальной и востребованной, так как ее решение обеспечит создание лучших инструментов по управлению умными устройствами.˜ отечественных и зарубежных источников позволил выделить и описать основные направления реализации системы с умными IoT датчиками, а также были инструменты, которые будут задействованы при ее проектировании.

1 АНАЛИЗ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

В ходе обзора литературных источников по тематике исследования было рассмотрено понятие облачных вычислений и их развитие, рассмотрены классификации облачных услуг, проанализированы существующие стандарты безопасности и организации, принимающие участие в разработке этих стандартов. Выполнен обзор наиболее известных поставщиков облачных услуг, рассмотрен российский рынок в период с 2014 г. по 2016 г. Составлен список основных угроз облачной безопасности и исследованы тенденции развития облачных вычислений.

В ходе системного анализа была сформирована цель проектирования, разработан список функций проектируемой системы:

- Ф1 — авторизация и аутентификация пользователей;
- Ф2 — сетевая защита;
- Ф3 — идентификация и обработка инцидентов связанных с безопасностью;
- Ф4 — предоставление доступа к услугам;
- Ф5 — мониторинг.

Выделены подсистемы:

а) подсистема аутентификации;
б) подсистема авторизации;
в) подсистема сетевой защиты;
г) подсистема проверки целостности данных.

Определена схема взаимодействия между подсистемами.

В соответствии с принципом функциональности составлена матрица инциденций функций системы и функций назначения подсистем. Произведена декомпозиция подсистем, определены стороны развития системы, определены события и действия, некорректные с точки зрения правил функционирования системы.

В ходе вариантного анализа сравнивались альтернативы гипервизоров (KVM, Hyper-V, VMware vSphere) в соответствии с критериями цены, масштабируемости, отказоустойчивости и интерфейсов управления. Построены матрицы парных сравнений второго и третьего уровня, исследованы согласованности матриц. Синтезированы глобальные приоритеты альтернатив. В результате анализа наибольшее предпочтение решено было отдать альтернативе B (VMware vSphere), однако для более точного определения гипервизора, необходимо сравнивать значительно большее число критериев.

В разделе описания облачной инфраструктуры представлены и описаны структурные схемы облачной инфраструктуры, а также архитектура системы безопасности.

В ходе экспериментальных исследований были проанализированы уязвимости 2016 г. в программном обеспечении, используемом в облачных вычислениях. Исследованы основные ошибки в программном коде продуктов и способы их исправления.

Эксплуатирована уязвимость CVE-2016-5195, в ходе которой удалось получить права суперпользователя сервера, предложены способы защиты от уязвимостей в ядре Linux.

Для мониторинга уязвимостей была написана программа, анализирующая данные из открытого источника уязвимостей. Данная программа может быть встроена в любую систему мониторинга и имеет возможность уведомлять системного администратора по Telegram.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы магистра были исследованы процессы обеспечения безопасности облачных сред.

В ходе исследования были проанализированы существующие проблемы и стандарты безопасности облачных вычислений, предложены способы решения данных проблем. Рассмотрена специфика предоставления облачных услуг зарубежных и отечественных поставщиков. Проанализированы наиболее опасные уязвимости за 2016 г.

В ходе системного анализа было описано системотехническое представление системы, описаны входные и выходные данные, составлен список функций системы безопасности, произведена декомпозиция системы и описана связь между ее элементами.

В ходе вариантного анализа был произведен сравнительный анализ гипервизоров между тремя альтернативами, в ходе которого был выбран наиболее оптимальный вариант.

В ходе экспериментальных исследования была эксплуатирована уязвимость CVE-2016-5195, благодаря которой локальный пользователь сервера получил доступ к правам суперпользователя. Скрипт не является законченным продуктом и распространяется под свободной лицензией.

Для мониторинга уязвимостей в программном обеспечении облачной среды был разработан скрипт на языке программирования Python. Скрипт осуществляет поиск по открытой базе уязвимостей согласно установленным параметрам. Программа находится в открытом доступе и распространяется под открытой лицензией.

Практическая значимость исследования состоит в возможности применения написанной программы в облачной среде провайдеров для анализа уязвимостей и незамедлительного реагирования на них. Также разработана защищенная облачная инфраструктура, описаны стратегии расширения инфраструктуры.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ЦОД — центр обработки данных

ПО — программное обеспечение

GNU — проект по разработке свободного программного обеспечения

GPL — General Public License, универсальная общественная лицензия

ОЗУ — оперативное запоминающее устройство

SSD — Solid State Drive, твердотельный накопитель

NIST — National Institute of Standards and Technology, Национальный институт стандартов и технологий

СХД — система хранения данных

SaaS — Software as a Service, программное обеспечение как услуга

PaaS — Platform as a Service, платформа как услуга

IaaS — Infrastructure as a Service, инфраструктура как услуга

ОС — операционная система

SOA — service-oriented architecture, сервис-ориентированная архитектура

AWS — Amazon Web Services

GCE — Google Compute Engine

OMG — Object Management Group

ИТ — информационные технологии

CSA — Cloud Security Alliance

DMTF — Distributed Management Task Force

SNIA — Storage Networking Industry Association

OGF — Open Grid Forum

OCC — Open Cloud Consortium

OASIS — Organization for the Advancement of Structured Information Standards

IETF — Internet Engineering Task Force, инженерный совет Интернета

ITU — International Telecommunications Union, Международный институт электросвязи

ETSI — European Telecommunications Standards Institute, Европейский институт телекоммуникационных стандартов

ANSI — American national standards institute, Американский национальный институт стандартов

IDPS — Intrusion Detection and Prevention Systems, руководство по системам обнаружения и предотвращения вторжений

EC2 — Elastic Compute Cloud, веб-сервис компании Amazon, предоставляющий вычислительные мощности в облаке

API — Application Programming Interface, интерфейс создания приложений

vCPU — Virtual Central Processing Unit, виртуальное процессорное ядро

AMI — Amazon Machine Images

EBS — Elastic Block Store, сервис постоянного хранилища блочного уровня для использования с инстансами Amazon

SPI — Secutiry Parameter Index, индекс параметра обеспечения безопасности

BGP — Border Gateway Protocol, протокол граничного шлюза

AS — автономная сетевая система

DNS — Domain Name System, система доменных имен

NTP — Network Time Protocol, протокол сетевого времени

SNMP — Simple Network Management Protocol, простой протокол сетевого управления

NDA — Non-disclosure agreement, соглашение о неразглашении

SSH — Secure Shell, безопасная оболочка

SQL — Structured Query Language, язык структурированных запросов

XSS — Cross-Site Scripting, межсайтовый скриптинг

VPN — Virtual Private Network, виртуальная частная сеть

МАИ — метод анализа иерархии

KVM — Kernel-based Virtual Machine, свободный гипервизор

ИС — индекс согласованности

СС — случайная согласованность

ОС — отношение согласованности

ЛПР — лицо принимающее решение

IoT — Internet of Things, интернет вещей

DDoS — Distributed Denial of Service, распределенная атака на отказ

SDN — Software-defined Networking, программно-определяемая сеть

CVE — Common Vulnerabilities and Exposures, словарь известных уязвимостей

ID — IDentificator, идентификатор

CVSS — Common Vulnerability Scoring System, система оценки уязвимостей

COW — Copy-on-write, копирование при записи

ARM — Advanced RISC Machine, усовершенствованная RISC-машина

GRUB — GRand Unified Bootloader, загрузчик операционной системы

JSON — JavaScript Object Notation, текстовый формат обмена данными

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Прудникова, А.А. Безопасность облачных вычислений / А.А. Прудникова // Мир телекома. – 2013. – №1. – С. 50-55.

2. Методические указания «Процедура системного анализа при проектировании программных систем» для студентов-дипломников дневной и заочной формы обучения специальности 7.091501 / Сост.: Сергеев Г.Г., Скатков А.В., Мащенко Е.Н. – Севастополь: Изд-во СевНТУ, 2005. – 32 с.

3. Методические указания к расчетно-графическому заданию на тему «Метод анализа иерархий» по дисциплине «Теория оптимальных решений» для студентов специальности 7.091501 «Компьютерные системы и сети» дневной и заочной формы обучения / Сост.: Ю.Н. Щепин – Севастополь: Изд-во СевНТУ, 2008. – 28 с.

4. Блюмин С.Л., Шуйкова И.А. Модели и методы принятия решений в условиях неопределенности. – Липецк: ЛЭГИ, 2001. – 138 с.

5. Hogan, M. NIST Cloud Computing Standarts Roadmap / M. Hogan, F. Liu, A. Sokol, J. Tong // NIST Special Publication 500-291, Version 2 Roadmap Working Group, 2013. – 113 с.

6. The 2016 Global Cloud Data Security Study. Ponemon Insitute LLC, 2016. – 40 с.

7. Беккер, М.Я. Информационная безопасность при облачных вычислениях: проблемы и перспективы / М.Я. Беккер, Ю.А. Гатчин, Н.С. Карманов-ский, А.О. Терентьев, Д.Ю. Федоров // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2011. – №1(71). – С. 97-102.

8. Емельянова, Ю.Г. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления / Ю.Г. Емельянова, В.П. Фраленко // Программные системы: теория и приложения. – 2011. – №4(8) – С. 17-31.

9. Chisnall, D. The Definitive Guide to the Xen Hypervisor / D. Chisnall. – 1st Edition // Prentice Hall Open Source Software Development, 2007. – 320 с.

10. Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» / Минкомсвязь России // Опубликован 12.02.2016 на официальном интернет-портале Министерства связи и массовых коммуникаций Российской Федерации

11. Облачные сервисы 2016 [Электронный ресурс] // CNews Analytics Режим доступа: https://goo.gl/cmDSMB (Дата обращения: 30.12.2016)

12. Cloud Security Alliance Releases 'The Treacherous Twelve' Cloud Computing Top Threats in 2016 [Электронный ресурс] // Cloud Security Alliance Research Group Режим доступа: https://goo.gl/l2aWLu (Дата обращения: 11.01.2017)

13. ИТ-инфраструктура предприятия 2010: Пути оптимизации [Электронный ресурс] // CNews Analytics Режим доступа: https://goo.gl/jzrrIO (Дата обращения: 05.01.2017)

14. Kaplan, J. Revolutionizing data center energy efficiency / J. Kaplan, W. Forrest, N. Kindler // Technical report, McKinsey & Company, 2008. – 15 с.

15. AWS signature version 1 is insecure [Электронный ресурс] // Daemonic Dispatches Режим доступа: https://goo.gl/70bggH (Дата обращения: 08.02.2017)

16. The CIS Critical Security Controls for Effective Cyber Defense [Электронный ресурс] // SANS website Режим доступа: https://goo.gl/pMjbNE (Дата обращения: 08.02.2017)

17. OWASP Top Ten Project [Электронный ресурс] // OWASP website Режим доступа: https://goo.gl/kSHOjF (Дата обращения: 08.02.2017)

18. CVE security vulnerability database. Security vulnerabilities, exploits, references and more [Электронный ресурс] // CVE Details. The ultimate security

vulnerability datasource Режим доступа: https://goo.gl/I3RtO2 (Дата обращения: 20.02.2017)

19. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel [Электронный ресурс] // CVE-2016-5195 info website Режим доступа: https://goo.gl/ziy3Nd (Дата обращения: 20.02.2017)

20. Bug 1355987 - (CVE-2016-6258, xsa182) CVE-2016-6258 xsa182 xen: x86: Privilege escalation in PV guests (XSA-182) [Электронный ресурс] // Red Hat Bugzilla Режим доступа: https://goo.gl/dlqtnR (Дата обращения: 20.02.2017)

21. CVE-2016-5696 [Электронный ресурс] // Common Vulnerabilities and Exposures. The Standart for Information Security Vulnerability Names Режим доступа: https://goo.gl/xYpFQQ (Дата обращения: 21.02.2017)

22. CVE-2016-5696 [Электронный ресурс] // Debian Security Bug Tracker Режим доступа: https://goo.gl/BXkTiL (Дата обращения: 21.02.2017)

23. CVE-2016-8655 - Red Hat Customer Portal [Электронный ресурс] // Red Hat Customer Portal Режим доступа: https://goo.gl/QhVbmm (Дата обращения: 21.02.2017)

24. CVE-2016-4997 [Электронный ресурс] // Common Vulnerabilities and Exposures. The Standart for Information Security Vulnerability Names Режим доступа: https://goo.gl/dbtXny (Дата обращения: 21.02.2017)

25. CVE-2016-4484: Cryptsetup Initrd root Shell [Электронный ресурс] // Hector Marco Gisbert - Lecturer and Cyber Security Researcher website Режим доступа: https://goo.gl/Jrfg6H (Дата обращения: 22.02.2017)

26. CVE-2016-1583 [Электронный ресурс] // Debian Security Bug Tracker Режим доступа: https://goo.gl/PIdqGR (Дата обращения: 22.02.2017)

27. gbonacini/CVE-2016-5195: A CVE-2016-5195 exploit example. [Электронный ресурс] // GitHub Режим доступа: https://goo.gl/9tFhHh (Дата обращения: 24.02.2017)

СПИСОК ИЛЛЮСТРАТИВНОГО МАТЕРИАЛА

СПИСОК ТАБЛИЧНОГО МАТЕРИАЛА

ПРИЛОЖЕНИЕ А

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕН

Программа мониторинга уязвимостей в программном обеспечении

ОПИСАНИЕ ПРОГРАММЫ

Листов — 3

2017

```
#!/usr/bin/env python3
# https://github.com/Amet13/vulncontrol

from sys import exit
from datetime import datetime
from urllib.parse import urlparse, urlencode
from urllib.request import urlopen, Request
from urllib.error import HTTPError
from json import loads
import argparse

today = datetime.now().strftime('%Y-%m-%d')

# Arguments parsing
parser = argparse.ArgumentParser()
parser.add_argument('-d', default=today, dest='DATE')
parser.add_argument('-m', default='1', dest='MINCVSS')
parser.add_argument('-t', default='', dest='TGTOKENID', nargs=2)
namespace = parser.parse_args()

try:
    tgtoken = namespace.TGTOKENID[0]
    tgid = namespace.TGTOKENID[1]
except(IndexError):
    tgtoken = ''
    tgid = ''

date = namespace.DATE
mincvss = namespace.MINCVSS
year = date.split('-')[0]
month = date.split('-')[1]

ids = []
cves = []
tgcves = []

```

```
# Maximum rows for one product
numrows = 30

tgurl = 'https://api.telegram.org/bot'
tgfull = '{0}{1}/sendMessage'.format(tgurl, tgtoken)
feedlink = 'https://www.cvedetails.com/json-feed.php'
source = open('products.txt', 'r')

# Getting product IDs from file
for line in source:
    if not line.startswith('#') and line.strip():
        parsed = urlparse(line)
        path = parsed[2]
        pathlist = path.split('/')
        ids.append(pathlist[2])
source.close()

# Get JSON
try:
    for x in ids:
        # Link example:
        # https://www.cvedetails.com/json-feed.php?product_id=47&
           month=02&year=2017&cvssscoremin=10&numrows=30
        link = '{0}?product_id={1}&month={2}&year={3}&cvssscoremin
           ={4}&numrows={5}' \
            .format(feedlink, x, month, year, mincvss, numrows)
        # Going to URL and get JSON
        getjson = urlopen(Request(link, headers={'User-Agent': '
           Mozilla'}))
        jsonr = getjson.read()
        for y in range(0, numrows):
            try:
                jp = loads(jsonr.decode('utf-8'))[y]
                if jp['publish_date'] == date:
                    result = '{0} {1} {2}' \
                        .format(jp['cve_id'], jp['cvss_score'], jp
                           ['url'])
```

```
                    tresult = 'CVSS: {0} URL: {1}' \
                        .format(jp['cvss_score'], jp['url'])
                    # Keep results in arrays
                    cves.append(result)
                    tgcves.append(tresult)
            except(IndexError):
                break
except(ValueError, KeyError, TypeError):
    print('JSON format error')

# Getting data for Telegram
tgdata = '{0} report:\n{1}'.format(date, '\n'.join(tgcves))
tgparams = urlencode({'chat_id': tgid, 'text': tgdata}).encode('utf
   -8')

if len(cves) == 0:
    print('There are no available vulnerabilities on ' + date)
    exit(0)
else:
    print('\n'.join(cves))
    if tgtoken == '' or tgid == '':
        print('Telegram alert did not sent')
        exit(1)
    else:
        try:
            urlopen(tgfull, tgparams)
            print('Telegram alert sent')
            exit(2)
        except(HTTPError):
            print('Telegram alert did not sent, check your token
               and ID')
            exit(3)
```