ORES
Научно-практический электронный журнал
**Оригинальные исследования (ОРИС)**, *ISSN 2222-0402*
www.ores.su
original-research.ru

**УДК 004.7**

# ОБЕСПЕЧЕНИЕ ИЗОЛЯЦИИ И УПРАВЛЕНИЯ СЕТЕВЫМ ТРАФФИКОМ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ МАЛОГО ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

**Владимир Алексеевич Раевский,**
ФГБОУ ВО «Калужский государственный университет им. К.Э. Циолковского», доцент кафедры «Информатики и информационных технологий», г. Калуга, var-77@mail.ru

**Мачехин Кирилл Витальевич**
ФГБОУ ВО «Калужский государственный университет им. К.Э. Циолковского», студент кафедры «Информатики и информационных технологий», г. Калуга, machekhinkv@studklg.ru

**Аннотация**

В статье анализируются требования технического задания одной из организаций г. Калуга (малое предприятие промышленной сферы) к изоляции и управлению изоляцией сетевого траффика. Проводится анализ существующих схем изоляции и обосновывается выбор схемы. Приводятся соответствующие настройки устройств сетевой инфраструктуры.

**Ключевые слова:** локальные вычислительные сети, изоляция траффика, уровни изоляции, управления изоляцией, виртуальные локальные сети (VLAN), списки контроля доступа (ACL).

# PROVIDING ISOLATION AND MANAGEMENT NETWORK TRAFFIC BETWEEN DIVISIONS SMALL INDUSTRIAL ENTERPRISE

**Vladimir A. Rayevsky,**
Kaluga State University named after K.E. Tsiolkovsky, Associate Professor of the Department of Informatics and Information Technologies, Kaluga, var-77@mail.ru

**Kirill V. Machekhin,**
Kaluga State University named after K.E. Tsiolkovsky, student of the Department of Informatics and Information Technologies, Kaluga, machekhinkv@studklg.ru

ABSTRACT

The article analyzes the requirements of the terms of reference of one of the organizations in Kaluga (a small industrial enterprise) for isolation and isolation management of network traffic. The analysis of the existing isolation schemes is carried out and the choice of the scheme is substantiated. The corresponding settings of network infrastructure devices are given.

**Keywords:** local area networks, traffic isolation, isolation levels, isolation management, Virtual Local Area Networks (VLANs), access control lists (ACLs).

1. Анализ технического задания Заказчика. Для административных подразделений одной из организаций г. Калуга, выпускающей электрооборудование, ранее были выбраны элементы проводной сетевой инфраструктуры [1].

В техническом задании Заказчика указано требование к изоляции сетевого траффика между подразделениями организации, расположенными на двух этажах здания ([1, Таблица 1]), с возможностью управления изоляцией.

Анализ показывает, что в одних областях изоляции должны находиться: «Отдел качества + Начальник отдела качества», «Директор + Приемная директора», «Отдел закупок + Начальник отдела закупок», «Технический отдел + Начальник технического отдела», «Бухгалтерия + Главный бухгалтер». Кроме того, в ранее спроектированной сетевой инфраструктуре находятся 37 телефонов VoIP-связи; авторами статьи [1] предлагается также осуществить снижение стоимости проекта за счет подключения VoIP-телефонии по мостовой схеме по схеме «Коммутатор ↔VoIP-телефон ↔ Рабочая станция».

2. Анализ и выбор схем изоляции сетевого траффика. Известны [2, 3 и др.] два варианта изоляции сетевого траффика: изоляция уровня L3 (иногда необоснованно называемая физической изоляцией) и изоляция уровня L2.

Для первого случая характерно наличие логических сетей (подсетей, в случае использования VLSM разбиения IP-адресов сетей), являющихся областями изоляции. Различные подразделения организации находятся в различных логических сетях; физически рабочие станции/VoIP-телефоны подразделения подключаются к центральному устройству – коммутатору, связывание в единую сетевую инфраструктуру происходит за счет маршрутизатора (устройства L3-уровня) или коммутатора с базовыми функциями маршрутизации (рис. 1) [2, 3, 6, 7].

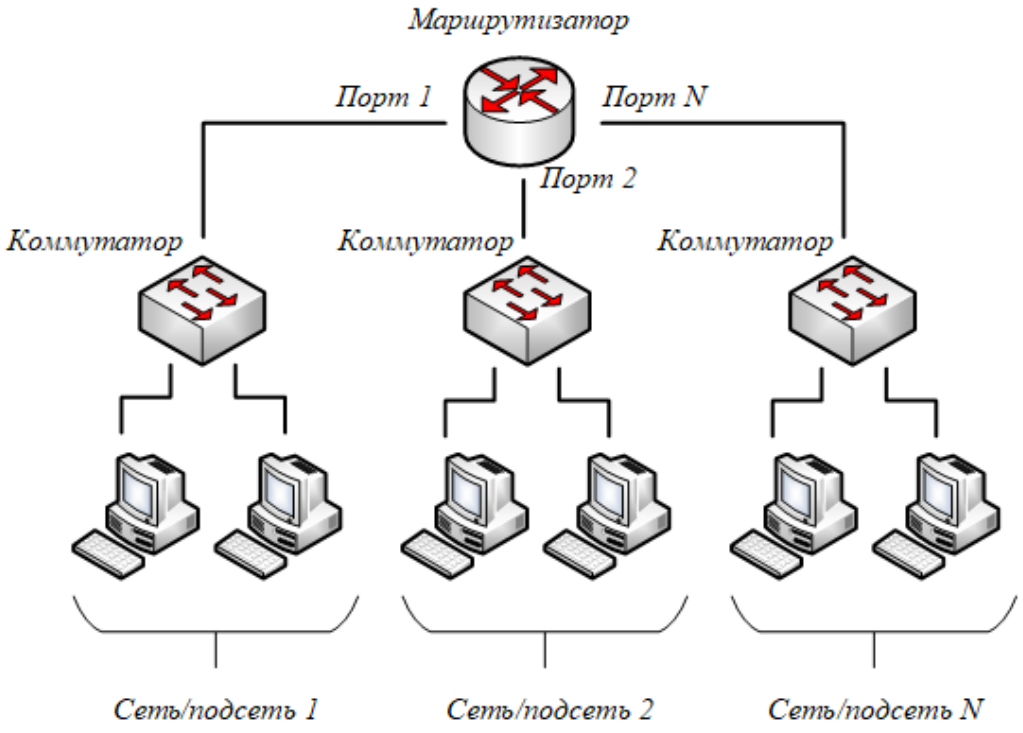


Рисунок 1 – Изоляция траффика на уровне L3

Если изменяется состав области изоляции (например, переход пользователя из одной сети/подсети в другую) необходимо будет осуществлять перекоммутацию рабочих станций/VoIP-телефонов на портах коммутаторов или на patch-панелях вплоть до прокладки новых кабелей витой пары. Таким образом, основной недостаток данной схемы – ее проблематичная масштабируемость. Известны также проблемы с защищенностью, изложенные в [8, 9]. К достоинствам следует отнести высокую надежность: в случае выхода из строя коммутатора одной из сетей/подсетей, остальные сегменты продолжат функционирование.

Исходя из вышесказанного, внедрение подобной схемы в перспективе может потребовать сравнительно большого объема работ с вероятностью возникновения ошибок. Особо отметим, что для реализации изоляции потребуется наличие маршрутизатора(ов) с количеством портов, соответствующим количеству областей изоляции.

Для второго случая (рис. 2) характерно применение технологии виртуальных локальных сетей (Virtual Local Area Networks, VLAN), позволяющей осуществлять группировку портов коммутатора по VLAN, и, как следствие, группировку (изоляцию) оконечных устройств [2 - 5]. Кадр, являющийся Protocol Data Unit на уровне L2 и промаркированный тегом соответствующей VLAN, будет передаваться только в той виртуальной сети, к которой принадлежит соответствующий порт коммутатора.

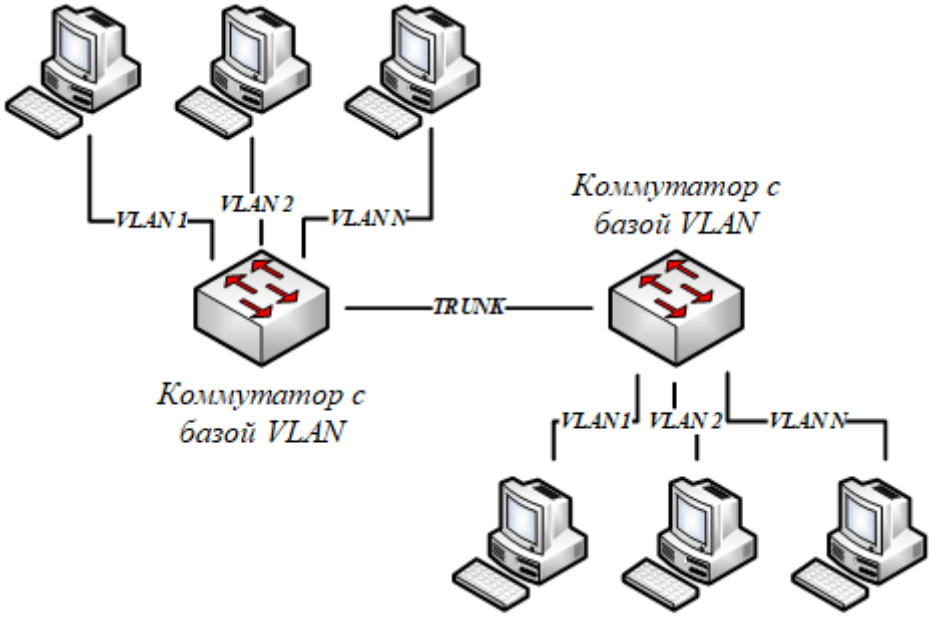


Рисунок 2 – Изоляция траффика на уровне L2

В случае наличия в сетевой инфраструктуре с VLAN двух и более коммутаторов для передачи тегированного траффика между следует применить на соответствующих портах технологию TRUNK [4, 5].

Для обеспечения управления изоляцией в данной схеме потребуется маршрутизатор или коммутатор с базовыми функциями маршрутизации (рис. 3). При этом существует возможность применить маршрутизатор с минимальным количеством портов: физическое подключение осуществляется одним кабелем витой пары к порту в режиме TRUNK, на котором разворачиваются логические подинтерфейсы («маршрутизатор на палочке»), обслуживающие маршрутизацию между VLAN, и, как следствие, дальнейшее управление изоляцией [4-7].

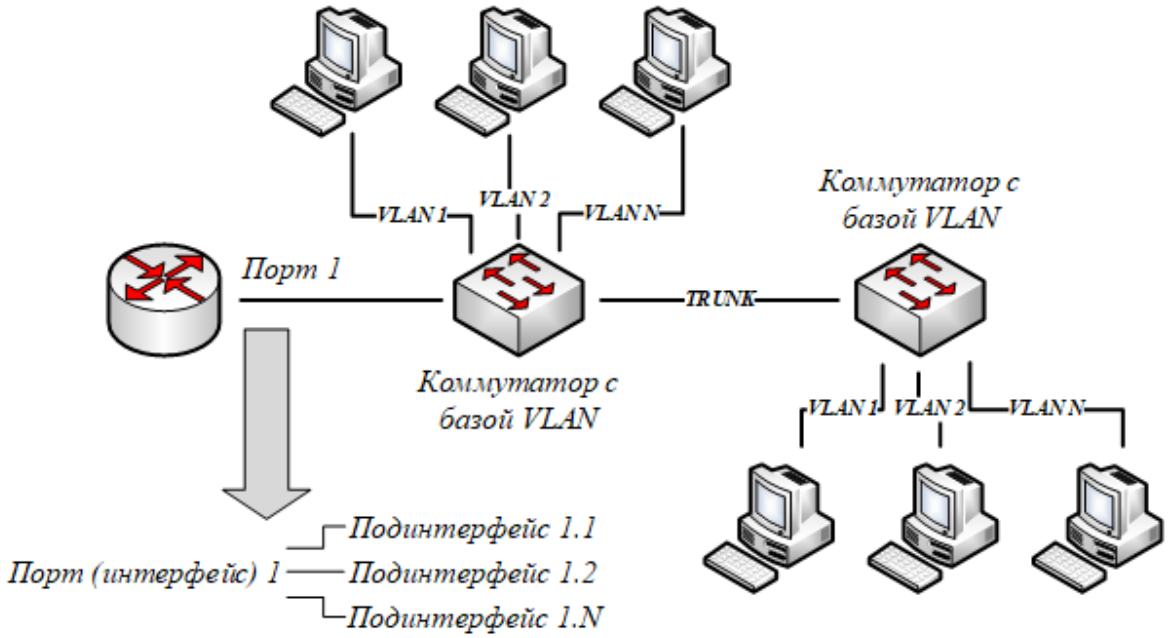


Рисунок 3 – Изоляция траффика на уровне L2 с маршрутизацией и управлением траффиком

К достоинствам данной схемы по сравнению с изоляцией на уровне L3 относится легкая масштабируемость инфраструктуры, уменьшение количества витой пары, снижение в сети широковещательного траффика. К недостаткам следует отнести необходимость в более дорогих коммутаторах, поддерживающих технологию VLAN.

Исходя из вышесказанного, учитывая выбор сетевого оборудования, описанный в [1], по согласованию с Заказчиком было решено применить изоляцию на уровне L2 посредством внедрения виртуальных локальных сетей.

3. Реализация изоляции траффика в спроектированной сетевой инфраструктуре посредством VLAN. В таблице 1 приведена сводная информация о подразделениях организации, name VLAN и id VLAN.

Таблица 1 – Разделение на VLAN

| № | Наименование помещения/подразделения | name VLAN | id VLAN |
|---|---|---|---|
| 1 | Офис | off | 5 |
| 2 | Охрана труда | ohr_trud | 10 |
| 3 | Служба по персоналу | hum_res | 20 |
| 4 | Офис лаборатории | of_lab | 30 |
| 5 | Отдел качества + Начальник отдела качества | otd_kach | 40 |
| 6 | Бухгалтерия + Главный бухгалтер | buh | 50 |
| 7 | Технический отдел + Начальник технического отдела | otd_teh | 60 |
| 8 | Отдел закупок + Начальник отдела закупок | otd_zak | 70 |
| 9 | Конференц-зал | conf_zal | 80 |
| 10 | - | print_share | 90 |

| | | | |
|---|---|---|---|
| 11 | Приемная директора + Директор | dir | 100 |
| 12 | IT-отдел | sys_admin | 110 |
| 13 | - | ip_voice | 115 |
| 14 | Сервер (Файловый сервер+контроллер домена) | serv | 2 |
| 15 | Сервер 1С: Предприятие | serv_1c | 3 |

К серверу, выполняющему роли файлового сервера и контроллера домена Active Directory, принтеру, расположенному в приемной директора, необходимо обеспечить доступ всем подразделениям на случай выхода из строя принтеров в подразделениях; к серверу 1С: Предприятие [10, 11] необходимо обеспечить доступ подразделениям «Бухгалтерия + Главный бухгалтер», «Отдел закупок + Начальник отдела закупок», «Служба по персоналу». Для реализации вышеназванных возможностей были созданы соответственно VLAN/id2/serv, VLAN/ id90/print_share и VLAN/ id3/serv_1c соответственно. В VLAN/id115/ip_voice изолированы VoIP-телефоны сотрудников организации. Управление изоляцией осуществляется за счет списков доступа на маршрутизаторе. На коммутаторах были развернуты базы VLAN; на рисунке 4 приведен пример листинга конфигурирования коммутатора WS-C2960L-24TS-LL по созданию VLAN для подразделений «Охрана труда» и «Служба по персоналу».

```
24TS(config)#vlan 10
24TS (config-vlan)#name ohr_trud
24TS (config-vlan)#exit
24TS (config)#vlan 20
24TS (config-vlan)#name hum_res
24TS (config-vlan)#exit
```

Рисунок 4 – Листинг создания VLAN для подразделений «Охрана труда» и «Служба по персоналу»

В таблице 2 приведены порты, переведенные в режиме ACCESS для каждой виртуальной локальной сети, а также порты TRUNK, обеспечивающие передачу тегированного траффика между коммутаторами и управляющим маршрутизатором.

Таблица 2 – Коммутаторы сетевой инфраструктуры и их порты в режиме ACCESS и TRUNK

| Порты в режиме ACCESS --- id VLAN | Порты в режиме TRUNK | IP-адреса и префиксы маски сетей |
|---|---|---|
| WS-C2960L-24TS-LL | | |
| Gi0/1 - Gi0/4 --- 5 | Gi0/24 | 192.168.5.0/24 |
| Gi0/5 - Gi0/7 --- 10 | | 192.168.10.0/24 |
| Gi0/8 - Gi0/11 --- 20 | | 192.168.20.0/24 |
| Gi0/12---80 | | 192.168.80.0/24 |
| Gi0/13---110 | | 192.168.110.0/24 |
| Gi0/14 - Gi0/17 --- 30 | | 192.168.30.0/24 |
| WS-C2960L-48TS-LL | | |
| Gi0/1 - Gi0/4 --- 40 | Gi0/47-Gi0/48 | 192.168.40.0/24 |
| Gi0/5-Gi0/6 --- 100 | | 192.168.100.0/24 |
| Gi0/7-Gi0/8 --- 90 | | 192.168.90.0/24 |

| | | |
|---|---|---|
| Gi0/9-Gi0/13 --- 50 | | 192.168.50.0/24 |
| Gi0/14-Gi0/20--- 60 | | 192.168.60.0/24 |
| Gi0/21-Gi0/32 --- 70 | | 192.168.70.0/24 |

Примечание: Gi - GigabitEthernet

На рисунке 5 приведен пример листинга конфигурирования портов коммутатора WS-C2960L-24TS-LL, переводящий их соответственно в режим ACCESS для VLAN подразделений «Охрана труда» и «Служба по персоналу» (с учетом количества рабочих станций и принтеров в подразделениях [1]), а также портов в состоянии TRUNK.

```
24TS (config)# interface range gigabitethernet 0/5-7
24TS (config-if-range)#switchport mode access
24TS (config-if-range)#switchport access vlan 10
24TS (config-if-range)#exit
24TS(config)#interface range gigabitethernet 0/8-11
24TS (config-if-range)#switchport mode access
24TS (config-if-range)#switchport access vlan 20
24TS (config-if-range)#exit
24TS (config)# interface gigabitethernet 0/24
24TS (config-if)#switchport mode trunk
24TS (config-if)#switchport trunk allowed vlan 5,10,20,30,40,50,60,70,80,90,100,110,115,2,3
24TS (config-if)#exit
```

Рисунок 5 – Листинг конфигурирования портов для подразделений «Охрана труда» и «Служба по персоналу» (режим ACCESS) и портов TRUNK

Аналогичным образом создавались все виртуальные локальные сети для подразделений в базе сетевых устройств и конфигурировались соответствующие порты. В результате все подразделения организации, сервер, выполняющий роли файлового сервера и контроллера домена, сервер с развернутым программным обеспечением «1С: Предприятие», IP-телефония и принтер, расположенный в приемной директора, были изолированы в соответствующих VLAN.

4. Реализация управления изоляцией траффика в спроектированной сетевой инфраструктуре посредством VLAN. На рисунке 6 приведен листинг конфигурирования порта маршрутизатора, обеспечивающего маршрутизацию траффика между виртуальными сетями организации (схема «маршрутизатор на палочке», рисунок 3). Коммутатор WS-C2960L-48TS-LL через порт Gi0/48 связан с портом маршрутизатора. На интерфейсе GigabitEthernet 0/1 были созданы соответствующие VLAN подинтерфейсы для передачи тегированного траффика; на каждом подинтерфейсе включено использование инкапсуляции dot1q.

```
RouterIn(config)#interface gigabitethernet 0/1.10
RouterIn (config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.10, changed state to up
RouterIn (config-subif)#encapsulation dot1Q 10
RouterIn (config-subif)#ip address 192.168.10.254 255.255.255.0
RouterIn (config-subif)#exit
RouterIn (config)# interface gigabitethernet 0/1.20
RouterIn (config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20, changed state to up
RouterIn (config-subif)#encapsulation dot1Q 20
RouterIn (config-subif)#ip address 192.168.20.254 255.255.255.0
RouterIn (config-subif)#exit
```

Рисунок 6 – Листинг конфигурирования подинтерфейсов маршрутизатора для обеспечения маршрутизации между виртуальными сетями

После настройки маршрутизации все VLAN будут иметь доступ друг к другу. Для управления изоляцией в соответствии с требованиями Заказчика были применены списки доступа, которые разрешают траффик, ограниченный правилами следующей схемы:

Запрещён трафик между виртуальными сетями.

Запрещен траффик между VLAN ip-voice и остальными VLAN.

Запрещен траффик между VLAN serv и глобальной сетью Интернет, VLAN serv_1c и глобальной сетью Интернет.

Разрешен траффик из виртуальных сетей off, ohr_trud, hum_res, of_lab, otd_kach, buh, otd_teh, otd_zak, conf_zal, dir, sys_admin к хосту общего принтера в приемной директора с IP-адресом 192.168.90.1 (VLAN print_share).

Разрешен траффик из всех виртуальных сетей к VLAN serv.

Разрешен траффик между сервером 1с и VLAN hum_res, buh, otd_zak, dir.

Как пример, на рисунке 7, а приведен листинг конфигурирования списков доступа для подразделения «Офис», на Рисунке 6, б – листинг конфигурирования списков доступа для подразделения «Служба по персоналу».

```
RouterIn(config-std-nacl)#ip access-list standard off
RouterIn(config-std-nacl)#permit host 192.168.90.1
RouterIn(config-std-nacl)#deny 192.168.10.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.20.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.30.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.40.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.50.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.60.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.70.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.80.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.90.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.100.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.110.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.115.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.7.0 0.0.0.255
RouterIn(config-std-nacl)#permit any
RouterIn(config-std-nacl)#exit
```

а)

```
RouterIn(config)#ip access-list standard hum_res
RouterIn(config-std-nacl)#permit host 192.168.90.1
RouterIn(config-std-nacl)#deny 192.168.30.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.40.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.50.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.60.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.70.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.80.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.90.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.100.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.110.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.115.0 0.0.0.255
RouterIn(config-std-nacl)#deny 192.168.7.0 0.0.0.255
RouterIn(config-std-nacl)#permit any
RouterIn(config-std-nacl)#exit
```

б)

Рисунок 7 – Листинг конфигурирования списков доступа для подразделения «Офис» (а) и «Служба по персоналу» (б)

Таким образом, требование технического задания Заказчика, описанного в [1], на изоляцию сетевого траффика между подразделениями организации и управление им реализовано полностью.

**Список литературы:**


1. Раевский В.А., Мачехин К.В. Обоснование выбора элементов проводной сетевой инфраструктуры для малого промышленного предприятия [Электронный ресурс]. // Научно-практический электронный журнал Оригинальные исследования (ОРИС). – 2022. – № 11. – С. 330-337. Режим доступа: https://ores.su/media/filer_public/2e/cd/2ecdf5c0-7c76-4c88-b401-b23f31596332/330-337.pdf.
2. Олифер В., Олифер Н. Компьютерные сети. Принципы технологии протоколы: Юбилейное издание. [Текст] / В. Олифер, Н. Олифер. – СПб.: Питер, 2020. – 1008 с.
3. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. [Текст] / Э. Таненбаум, Д. Уэзеролл. – СПб.: Питер, 2012. – 960 с.
4. David H. CCNP SWITCH 642-813. Official Certification Guide. [Текст] / H. David. – Indianapolis: Cisco Press, 2010. – 512 с.
5. Леммл Т., Хейлз К. CCNP. Настройка коммутаторов Cisco. Учебное руководство. [Текст] / Т. Леммл, К. Хейлз. – М.: «Лори», 2002. – 464 с.
6. Odom W. CCNP ROUTE 642-902 Official Certification Guide. [Текст] / W. Odom – Indianapolis: Cisco Press, 2010. – 920 с.
7. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация. [Текст] / У. Одом – М.: ООО «И.Д. Вильямс», 2015. – 736 с.
8. Ткаченко А.Л., Бурцева В.В., Кузнецова В.И. Анализ проблем защиты организации от межсетевых атак // Дневник науки. – 2021. – № 8 (56). – Порядковый номер статьи 21.
9. Ткаченко А. Л., Гордеева А. Ю., Шавренко А. В. Имитационное моделирование распространения кибератак на промышленные предприятия / // Инновационные технологии, экономика и менеджмент в промышленности: Сборник научных статей по итогам IV международной научной конференции, Волгоград, 22–23 апреля 2021 года. – Волгоград: Общество с ограниченной ответственностью «КОНВЕРТ», 2021. – С. 238-240.
10. Ткаченко А.Л., Копнева В.В. Анализ и интеграция информационной системы предприятия с облачным сервисом // вестник калужского университета. – 2021. – №3. – С. 42-45.
11. Ткаченко А.Л., Рожкова В.А., Леонова В.Д., Щеглова А.А. Реинжиниринг бизнес-процессов компании ООО «Компьютерра» за счет внедрения конфигурации «1с: Управление торговлей» // Информационные технологии в экономике и управлении. Сборник материалов IV Всероссийской научно-практической конференции (с международным участием). – 2020. – С. 126-129.

**References:**

1. Raevsky V.A., Machekhin K.V. Justification for choosing of elements of wired network infrastructure for a small industrial enterprise. [Electronic resource] // The electronic scientific & practical journal ORIS. – 2022. – № 11. – P. 330-337. Access mode: https://ores.su/media/filer_public/2e/cd/2ecdf5c0-7c76-4c88-b401- b23f31596332/330-337.pdf. (in Russian).
2. Olifer V., Olifer N. Komp'yuternye seti. Principy tekhnologii protokoly: YUbilejnoe izdanie. [Text] / V. Olifer, N. Olifer. – Saint Petersburg.: Piter, 2020. – 1008 p. (in Russian).
3. Tanenbaum E., Uezeroll D. Komp'yuternye seti. 5-e izd. [Text] / E. Tanenbaum, D. Uezeroll. – Saint Petersburg: Piter, 2012. – 960 p. (in Russian).
4. David H. CCNP SWITCH 642-813. Official Certification Guide. [Text] / H. David. – Indianapolis: Cisco Press, 2010. – 512 p.
5. Lemml T., Hejlz K. CCNP. Nastrojka kommutatorov Cisco. Uchebnoe rukovodstvo. [Text] / T. Lemml, K. Hejlz. – Moscow: «Lori», 2002. – 464 p. (in Russian).
6. Odom W. CCNP ROUTE 642-902 Official Certification Guide. [Text] / W. Odom – Indianapolis: Cisco Press, 2010. – 920 p.
7. Odom U. Oficial'noe rukovodstvo Cisco po podgotovke k sertifikacionnym ekzamenam CCNA ICND2 200-101: marshrutizaciya i kommutaciya. [Text] / U. Odom – Moscow: LTD «I.D. Vil'yams», 2015. – 736 p. (in Russian).
8. Tkachenko A.L., Burceva V.V., Kuznecova V.I. Analiz problem zashchity organizacii ot mezhsetevyh atak // Dnevnik nauki. – 2021. – № 8 (56). – article number 21. (in Russian).
9. Tkachenko A. L., Gordeeva A. YU., SHavrenko A. V. Imitacionnoe modelirovanie rasprostraneniya kiberatak na promyshlennye predpriyatiya // Innovacionnye tekhnologii, ekonomika i menedzhment v promyshlennosti: Sbornik nauchnyh statej po itogam IV mezhdunarodnoj nauchnoj konferencii, Volgograd, 22–23 aprelya 2021 goda. – Volgograd: LTD «KONVERT», 2021. – P. 238-240. (in Russian).
10. Tkachenko A.L., Kopneva V.V. Analiz i integraciya informacionnoj sistemy predpriyatiya s oblachnym servisom // Vestnik kaluzhskogo universiteta. – 2021. – №3. – P. 42-45. (in Russian).
11. Tkachenko A.L., Rozhkova V.A., Leonova V.D., Shcheglova A.A. Reinzhiniring biznes-processov kompanii OOO «Komp'yuterra» za schet vnedreniya konfiguracii «1C: Upravlenie torgovlej» // Informacionnye tekhnologii v ekonomike i upravlenii. Sbornik materialov IV Vserossijskoj nauchno-prakticheskoj konferencii (s mezhdunarodnym uchastiem). – 2020. – P. 126-129. (in Russian).