

**ДВОРЕЦКАЯ П.С., БАЗАРОВА И. А.  
ЗАЩИЩЕННАЯ ДОВЕРЕННАЯ СРЕДА ПЕРЕДАЧИ ИНФОРМАЦИИ  
С ИСПОЛЬЗОВАНИЕМ ПРОДУКТОВ ViPNET ДЛЯ ФИЛИАЛА  
ООО «ГАЗИНФОРМСЕРВИС» В Г. УХТА**

*УДК 004.056, ГРНТИ 81.93.29*

Защищенная доверенная среда передачи информации с использованием продуктов ViPNet для филиала ООО «Газинформсервис» в г. Ухта

Secure trusted information transmission environment using ViPNet products for the branch of Gazinformservice LLC in Ukhta

**П. С. Дворецкая<sup>1</sup>, И. А. Базарова<sup>2</sup>**

**P. S. Dvoretzkaya<sup>1</sup>, I. A. Bazarova<sup>2</sup>**

<sup>1</sup> ООО «Газинформсервис», г. Ухта;  
<sup>2</sup> Ухтинский государственный технический университет, г. Ухта

<sup>1</sup>Gazinformservice LLC in Ukhta  
<sup>2</sup>Ukhta State Technical University, Ukhta

*Данная статья посвящена разработке макета защищенной сети, объединяющей центральный офис и филиал ООО «Газинформсервис». Развертывание макета осуществлялось с применением продуктов ViPNet, обеспечивающих безопасную передачу данных по общедоступной сети путем организации виртуальных частных сетей (VPN)*

*This article is devoted to the development of a layout of a secure network that unites the central office and a branch of Gazinformservice LLC. The layout was deployed using ViPNet products that provide secure data transmission over a public network by organizing virtual private networks (VPN)*

**Ключевые слова:** ViPNet, VPN, информационная безопасность, макетирование

**Keywords:** ViPNet, VPN, information security, layout

## **Введение**

В целях повышения эффективности и безопасности хранения информации современные компании переходят от обмена бумажными документами к электронному документообороту, использованию облачных хранилищ и серверов приложений. Зачастую различные отделы или филиалы одного предприятия могут располагаться далеко друг от друга или компания сотрудничает с другой, не связанной с ней единой сетью.

Как правило компании для передачи коммерческой и управленческой информации стремятся использовать общедоступную сеть Интернет в силу дешевизны и доступности такого решения. В следствие чего защита персональных и иных конфиденциальных данных в процессе их передачи по сети становится все более актуальной задачей.

Наиболее распространенным способом обеспечения безопасности при передаче данных через Интернет является технология виртуальных частных сетей (VPN). VPN позволяет создать защищенный туннель между устройствами, что обеспечивает конфиденциальность и целостность передаваемых данных.

### **Предпроектное исследование**

ООО «Газинформсервис» является компанией-подрядчиком, специализирующейся на системном интегрировании в области корпоративной информационной безопасности и создании инженерно-технических решений для защиты информации.

В региональном подразделении компании, находящемся в городе Ухта, реализовано взаимодействие с центральным офисом компании, расположенным в Санкт-Петербурге.

Филиал предприятия, как многие другие компании, занимается обработкой, хранением и передачей различного рода информации, в том числе относящейся к конфиденциальной, то есть имеющей ограниченный доступ в соответствии с законодательством.

Во избежание утечек конфиденциальной информации, ее искажения и несанкционированного использования необходимо применение различных мер защиты информации, как внутри локальной сети, так и при межсетевом взаимодействии.

Перед организацией защиты от внешних атак необходимо принять во внимание атаки со стороны внутреннего нарушителя, который, являясь сотрудником компании, может заниматься хищением, искажением и несанкционированной передачей данных и подвергнуть опасности локальную сеть предприятия.

В качестве мер для защиты локальной сети предприятия применяются следующие технические средства:

– DLP-системы (Data Leak Prevention – Предотвращение Утечки Данных) – основной принцип работы заключается перехвате и анализе данных, передаваемых внутри корпоративной сети и за ее пределы. В случае если информация переносится на какой-либо носитель или пересылается тому пользователю, который не должен иметь к ней доступ, происходит блокировка передачи.

– корпоративное антивирусное программное обеспечение (Kaspersky) для снижения рисков проникновения в локальную сеть предприятия вредоносного программного обеспечения.

– система защиты от несанкционированного доступа («Блокхост-сеть») – средство контроля съёмных машинных носителей информации и защиты от несанкционированного доступа ресурсов рабочих станций и серверов. мм

Взаимодействие филиала компании и центрального офиса происходит с использованием сети Интернет. Данный участок сети считается наиболее уязвимым, так как возможны различные атаки со стороны злоумышленников, проникновение вредоносного программного обеспечения.

Для защиты от несанкционированного доступа в каждую из подсетей, а также возможных атак на границах подключения как главного офиса, так и филиала, к общедоступной сети установлены аппаратные межсетевые экраны Cisco ASA 5505, на основе которых реализуется не только фильтрация проходящего трафика, но и построение туннелей через публичную сеть, то есть реализуется VPN.

Однако для передачи персональных данных по каналам связи, которые выходят за пределы контролируемой зоны, должны применяться сертифицированные средства криптографической защиты информации (СКЗИ). Под контролируемой зоной понимается область, территория, на которой запрещено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Кроме того, в соответствии с политикой импортозамещения необходимо использование отечественного программного и аппаратного обеспечения.

В связи с имеющимися угрозами безопасности и необходимостью замены оборудования актуальным становится разработка системы защиты обмена данными между центральным офисом и филиалом. Необходима разработка макета, с помощью которого будет смоделирована работа сети и проверена ее работоспособность.

Основной технологией обеспечения безопасности передачи является VPN, так как это единственное средство, при помощи которого возможно осуществлять передачу данных между различными удаленными сегментами сети с должным уровнем защиты.

Реализация VPN может производиться как с использованием собственного оборудования и ПО, так и комплекса услуг и оборудования Интернет-провайдера. Использование VPN как услуги возможно в том случае, если удаленные офисы подключены через одного Интернет-провайдера.

Так как головной офис рассматриваемой компании находится в г. Санкт-Петербург, а филиал – в г. Ухта используются различные провайдеры, поэтому применение VPN как услуги не представляется возможным. Кроме того, при нахождении отделений компании в разных городах или даже странах с трудом удастся найти провайдера, который сможет предоставить требуемый уровень защищенности данных и скорости передачи за оптимальную стоимость.

Поэтому решением в данном случае является организация защищенной доверенной сети между удаленными офисами компании «Газинформсервис» с применением собственного оборудования и специализированного программного обеспечения.

На российском рынке представлен целый ряд отечественных продуктов для развертывания сети VPN.

Однако в связи с политикой рассматриваемой компании создание защищенной среды передачи информации необходимо осуществить с применением продуктов «ViPNet», производимой компанией ОАО «ИнфоТеКС».

Основные продукты линейки, которые были использованы для развертывания защищенной частной сети:

– ViPNet Administrator – программный комплекс, предназначенный для управления виртуальной сетью ViPNet.

– ViPNet Coordinator – шлюз безопасности, предназначенный для обеспечения безопасной передачи данных между защищенными сегментами виртуальной сети ViPNet, а также фильтрации IP-трафика.

– ViPNet Client – программное обеспечение, обеспечивающее защиту клиентских компьютеров от несанкционированного доступа при работе в глобальных и локальных сетях.

– ViPNet xFirewall – межсетевой экран следующего поколения (NGFW), выполняющий фильтрацию трафика на сетевом и транспортном уровнях модели OSI (с контролем состояния сессий).

При реализации макета защищенной сети предприятия были использованы виртуальные координаторы и межсетевые экраны. Данное решение позволяет провести тестирование оборудования перед реальной закупкой программно-аппаратного комплекса.

### Реализация макета защищенной сети

Перед реализацией стенда защищенной сети были построены схемы физического и сетевого уровней (Рисунки 1 и 2).

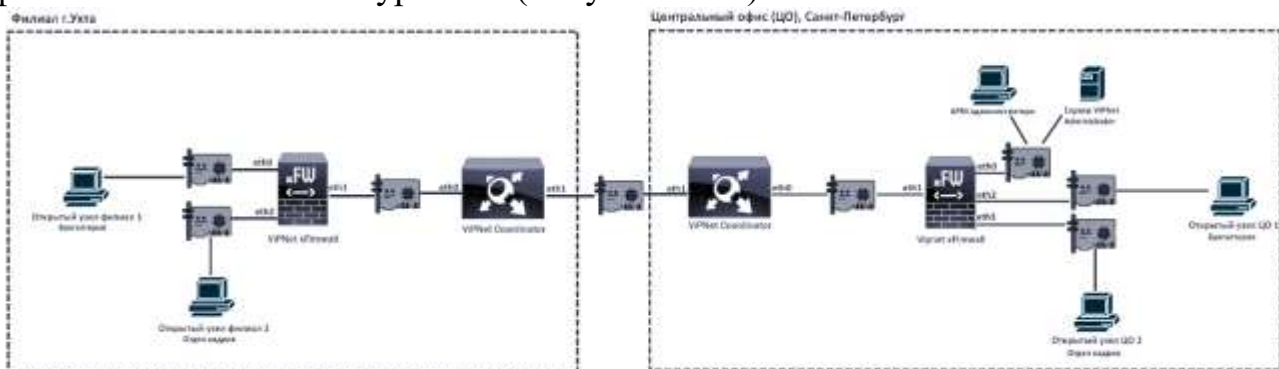


Рисунок 1. Схема макетируемой сети. Физический уровень

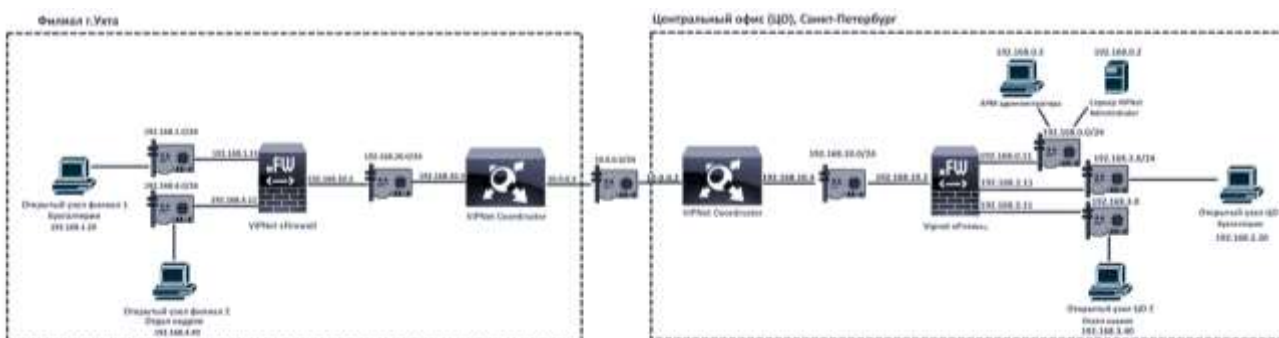


Рисунок 2. Схема макетируемой сети. Сетевой уровень

Все сетевые узлы были связаны между собой сетевыми адаптерами виртуальных машин. Развертывание стенда производилось в среде виртуализации VMWare Workstation.

Работы по развертыванию макета сети производились в следующем порядке:

- Создание виртуальной машины (VM) сервера ViPNet Administrator на базе Windows Server 2016, развертывание ViPNet Administrator – установка серверной и клиентской части ЦУС и УКЦ, установка ViPNet Client.

- Создание структуры сети в ЦУС, выдача дистрибутивов ключей на все узлы сети.

- Развертывание АРМ администратора сети на базе Windows 10 – установка клиентской части ЦУС и ViPNet Client.

- Развертывание 2 VM координаторов – ViPNet Coordinator VA 4.3.3. Проведение первичной настройки, установка дистрибутива ключей, назначение адресов физическим интерфейсам в соответствии со схемой сети.

- Развертывание 2 VM межсетевых экранов – ViPNet xFirewall VA 5.3.0. Проведение первичной настройки, установка дистрибутива ключей, назначение адресов физическим интерфейсам в соответствии со схемой сети.

- Настройка маршрутизации между узлами сети.

- Развертывание VM открытых узлов конечных пользователей на базе Windows 10. Настройка адресов в соответствии со схемой сети.

- Настройка туннелей между открытыми узлами при помощи ViPNet Administrator.

- Настройка правил межсетевого экранирования.

- Проверка связности открытых узлов.

### **Результаты разработки**

Результатом разработки стал стенд, состоящий из 11 виртуальных машин, между которыми организовано сетевое взаимодействие.

Между открытыми узлами отделов бухгалтерии и отдела кадров, то есть пользовательскими компьютерами, на которых не установлено ПО ViPNet, организовано построение VPN-туннелей и шифрование передаваемых данных.

Для проверки защищенности соединения был снят дамп трафика с внутреннего и внешнего сетевых интерфейсов координатора центрального офиса.

Под внешним подразумевается сетевой интерфейс eth1, направленный в сторону в сторону сети Интернет, где находится координатор филиала, тогда как под внутренним – сетевой интерфейс eth0, направленный в локальную сеть компании.

Дамп трафика был снят с координатора при помощи встроенного инструмента «tcpdump» с записью в файл с расширением «.pcap». Затем содержимое данных файлов было просмотрено при помощи анализатора трафика Wireshark. Результаты представлены на рисунках 3 и 4.

Для проверки защищенности трафика производилось удаленное редактирование файла «Worker info.txt», находящегося в папке общего доступа в подсети отдела кадров.

В случае с трафиком, снятым с внутреннего интерфейса координатора, удастся просмотреть параметры пакетов, такие как адреса источников и получателей, типы отправляемых сообщений и используемые протоколы. В

данном случае передача данных происходила по протоколу SMB.

Кроме того, было отображено и само содержимое передаваемых сообщений, в данном случае был виден текст удаленно редактируемого документа – ФИО работника, паспортные данные и ИНН.

No.	Time	Source	Destination	Protocol	Length	Info
60	26.193156	192.168.4.40	192.168.3.40	TCP	54	49752 → 445 [ACK] Seq=5793 Ack=6825 Win=257 Len=0
61	26.193277	192.168.4.40	192.168.3.40	SMB2	162	SetInfo Request FILE_INFO/SMB2_FILE_ALLOCATION_INFO
62	26.193313	192.168.4.40	192.168.3.40	SMB2	154	Notify Request
63	26.194955	192.168.4.40	192.168.3.40	TCP	54	49752 → 445 [ACK] Seq=6001 Ack=6971 Win=257 Len=0
64	26.195328	192.168.4.40	192.168.3.40	SMB2	286	Create Request File:
65	26.196886	192.168.4.40	192.168.3.40	SMB2	260	Find Request SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern
66	26.198857	192.168.4.40	192.168.3.40	SMB2	146	Close Request
67	26.200683	192.168.4.40	192.168.3.40	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO
68	26.206907	192.168.4.40	192.168.3.40	SMB2	230	Write Request Len:60 Off:0
69	26.266069	192.168.4.40	192.168.3.40	TCP	54	49752 → 445 [ACK] Seq=6815 Ack=8227 Win=252 Len=0
70	27.139747	192.168.4.40	192.168.3.40	SMB2	234	Create Request File: Worker info.txt
71	27.143211	192.168.4.40	192.168.3.40	SMB2	146	Close Request
72	27.197243	192.168.4.40	192.168.3.40	SMB2	382	Create Request File: desktop.ini
73	27.200241	192.168.4.40	192.168.3.40	SMB2	171	Read Request Len:46 Off:0
74	27.266965	192.168.4.40	192.168.3.40	TCP	54	49752 → 445 [ACK] Seq=7532 Ack=9029 Win=255 Len=0
75	28.188268	192.168.4.40	192.168.3.40	SMB2	154	Notify Request
76	28.265761	192.168.4.40	192.168.3.40	TCP	54	49752 → 445 [ACK] Seq=7632 Ack=9106 Win=254 Len=0
77	29.077332	11.0.0.6	192.168.10.3	UDP	43	2046 → 2046 Len=1

> Frame 68: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits)

▼ Ethernet II, Src: VMware\_d2:b6:e8 (00:0c:29:d2:b6:e8), Dst: VMware\_3c:0b:32 (00:0c:29:3c:0b:32)

> Destination: VMware\_3c:0b:32 (00:0c:29:3c:0b:32)

> Source: VMware\_d2:b6:e8 (00:0c:29:d2:b6:e8)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.4.40, Dst: 192.168.3.40

> Transmission Control Protocol, Src Port: 49752, Dst Port: 445, Seq: 6639, Ack: 8143, Len: 176

```

0000  00 0c 29 3c 0b 32 00 0c 29 d2 b6 e8 08 00 45 00  ..<2..).....E.
0010  00 d8 50 76 00 00 7d 06 64 09 c0 a8 04 28 c0 a8  ..Pv..}..d....(..
0020  03 28 c2 58 01 bd 67 79 60 03 ba 46 e5 73 50 18  ..(X..gy`..F..sP.
0030  00 fc 89 6b 00 00 00 00 00 ac fe 53 4d 42 40 00  ...k.....SMB@.
0040  01 00 00 00 00 00 09 00 01 00 30 00 00 00 00 00  .....0.....
0050  00 00 39 03 00 00 00 00 00 00 ff fe 00 00 05 00  ..9.....
0060  00 00 5d 00 00 04 00 08 00 00 00 00 00 00 00 00  ..].....
0070  00 00 00 00 00 00 00 00 00 00 31 00 70 00 3c 00  .....1.p.<.
0080  00 00 00 00 00 00 00 00 00 00 eb 04 00 00 02 00  .....eb0400000200
0090  00 00 f1 00 20 00 02 00 00 00 00 00 00 00 00 00  .....
00a0  00 00 00 00 00 00 00 00 00 00 46 49 4f 20 49 76  .....FIO Iv
00b0  61 6e 6f 76 20 49 76 61 6e 20 49 76 61 6e 6f 76  anov Iva n Ivanov
00c0  69 63 68 0d 0a 50 61 73 73 70 6f 72 74 20 38 37  ich..Pas sport 87
00d0  31 35 20 37 32 32 31 35 36 0d 0a 49 4e 4e 20 32  15 72215 6..INN 2
00e0  32 32 32 32 32 32                                     222222

```

Содержимое редактируемого файла

Рисунок 3. Открытый трафик, снятый с внутреннего интерфейса

Трафик, снятый с внешнего интерфейса, выглядит иначе: передаваемые пакеты инкапсулированы в протокол IPv4, что скрывает реальные протоколы передачи данных.

В качестве отправителя и получателя указаны белые адреса внешних интерфейсов координаторов, что скрывает реальную структуру сети.

Кроме того, содержимое пакетов зашифровано, что исключает возможность хищения конфиденциальных сведений, их анализа, модификации.

Проведя анализ трафика, можно убедиться, что передаваемые между сегментами сети сведения защищены от перехвата, поскольку происходит построение VPN-туннелей и шифрование отправляемых данных.

```

19 4.587289      10.0.0.2      10.0.0.3      IPv4      191 Unknown (241)
20 10.184615     10.0.0.2      10.0.0.3      IPv4      411 Unknown (241)
21 10.186925     10.0.0.2      10.0.0.3      IPv4      181 Unknown (241)
22 10.186963     10.0.0.2      10.0.0.3      IPv4      187 Unknown (241)
23 10.188559     10.0.0.2      10.0.0.3      IPv4      111 Unknown (241)
24 10.188645     10.0.0.2      10.0.0.3      IPv4      181 Unknown (241)
25 10.188844     10.0.0.2      10.0.0.3      IPv4      187 Unknown (241)
26 10.190922     10.0.0.2      10.0.0.3      IPv4      1019 Unknown (241)
27 10.192853     10.0.0.2      10.0.0.3      IPv4      239 Unknown (241)
28 10.194640     10.0.0.2      10.0.0.3      IPv4      243 Unknown (241)
29 10.199273     10.0.0.2      10.0.0.3      IPv4      195 Unknown (241)
30 11.031069     10.0.0.2      192.168.20.2  UDP      708 55777 → 55777 Ler
31 11.229837     10.0.0.2      10.0.0.3      IPv4      1019 Unknown (241)

```

---

```

> Frame 8: 299 bytes on wire (2392 bits), 299 bytes captured (2392 bits)
✓ Ethernet II, Src: VMware_d2:b6:f2 (00:0c:29:d2:b6:f2), Dst: VMware_4d:d3:e4 (00:0c:29:4d:d3:e4)
  > Destination: VMware_4d:d3:e4 (00:0c:29:4d:d3:e4)
  > Source: VMware_d2:b6:f2 (00:0c:29:d2:b6:f2)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.3
> Data (265 bytes)

```

---

```

0000  00 0c 29 4d d3 e4 00 0c 29 d2 b6 f2 08 00 45 00  ..)M.... ).....E.
0010  01 1d 2e d7 00 00 7e f1 f8 14 0a 00 00 02 0a 00  .....~w.....
0020  00 03 96 22 d6 8f 8a 03 79 36 34 e1 1c 32 68 da  .."....y64..2h.
0030  59 66 45 40 a6 2e 7e 18 4d 05 df 7e ed 58 98 61  YfE@.~.M...X.a
0040  27 51 e9 10 c7 01 95 45 4b 92 23 a7 41 3a 74 74  'Q....E K.#:A:tt
0050  10 8f 6c b0 a8 8a 39 22 9c 3d ad 6b a0 15 3c f5  ..1...9" .=k.<<.
0060  95 33 3f c2 aa 0a b4 ca 2a f5 91 75 f2 a9 6f 45  ..3?.....*..u...oE
0070  f3 8d 33 d1 82 5f da 55 0b 82 53 c8 b0 5a a7 9e  ..3..._U ..S..Z..
0080  b1 1e 1c 5d c6 8f 56 83 38 ba d3 10 d3 a1 0e 66  ...]..V. 8.....f
0090  f9 18 aa 65 79 fd 61 00 c2 ed 24 55 1a e6 0e 3f  ...ey.a. ..$U...?
00a0  8d 50 00 b3 f0 5c f3 5e 25 d5 1f 29 8e 78 52 50  .P...\.^ %..).xRP
00b0  12 c0 89 37 a7 52 7f e0 4f ac a4 63 c0 dc 58 a5  ...7.R.. 0..c..X.
00c0  70 a4 a5 63 f0 2a d8 38 7a f0 2c 47 9f db 77 34  p..c.*.8 z.,G..w4
00d0  00 34 41 52 07 a7 e2 f7 06 40 61 8e 9c 1f 22 79  .4AR.... @a..."y
00e0  e7 fc 15 a7 7f 7c f2 c6 f9 92 61 4f 67 d1 4c 0d  ....|.. ..a0g.L.
00f0  32 d4 33 6c 41 0c ab eb 33 29 6d f3 c3 c2 d7 13  2.3lA... 3)m.....
0100  19 14 13 29 e6 35 50 27 00 0c 88 ff ff ff fe 00  ...).5P' .....
0110  20 15 76 e7 0e cd ce 31 13 a3 1f 64 37 00 00 00  .v...1 ...d7...
0120  00 50 27 00 0a 14 0b 49 4c 34 31

```

Рисунок 4. Зашифрованный трафик, снятый с внешнего интерфейса

## Заключение

В данной статье дано краткое описание работ по разработке и проектированию макета защищенной сети, построенного на основе продуктов ViPNet.

В рамках разработки был произведен анализ предметной области и выявлена необходимость в построении защищенной среды передачи информации на основе отечественного программного и аппаратного обеспечения для построения VPN сетей.

В ходе работ была произведена настройка программного и программно-аппаратного обеспечения ViPNet.

Результатом работы стал виртуальный стенд защищенной сети. Для безопасной передачи данных между открытыми узлами сети были подняты VPN-

туннели. Также была совершена проверка работоспособности и безопасности развернутой сети. При помощи анализатора трафика Wireshark удалось убедиться в защищенности передаваемых данных.

Таким образом, использование продуктов ViPNet и в целом технологии VPN является способом повышения безопасности передачи данных в общедоступных сетях и позволяет избежать успешной реализации атак, направленных на перехват данных, их анализ и хищение.

### **Список использованных источников и литературы**

1 Аникин, Д. В. Защита информации в корпоративной сети с использованием технологии VPN / Д. В. Аникин. – Текст : электронный // Банковский бизнес и финансовая экономика: глобальные тренды и перспективы развития. – 2021. № 3. – С. 21-26.

2 Курсаков, О.В., Титов В.В., Емельянова М.М. Экспериментальное исследование эффективности защиты данных в беспроводной локальной сети Wi-Fi с помощью технологии ViPNet / О.В. Курсаков, В.В. Титов, М.М. Емельянова – Текст: электронный // Информационные технологии в науке, промышленности и образовании. Сборник трудов Всероссийской научно-технической конференции. Ижевск, 2020. – С. 166–172.

3 Линейка продуктов VipNet [Электронный ресурс]. – Режим доступа: <https://infotecs.ru/product/> (дата обращения: 26.02.2023).

4 Чефранова А.О. Технология построения VPN ViPNet: курс лекций: Учебное пособие. – Москва: Прометей, 2009. – 180 с.

### **List of references**

1 Anikin, D. V. Information protection in a corporate network using VPN technology / D. V. Anikin. – Text : electronic // Banking business and financial economics: global trends and development prospects. 2021. No 3. PP. 21-26.

2 Kursakov, O.V., Titov V.V., Emelyanova M.M. Experimental study of the effectiveness of data protection in a wireless LAN Wi-Fi using ViPNet technology / O.V. Kursakov, V.V. Titov, M.M. Emelyanova Text: electronic // Information technologies in science, industry and education. 2020. PP. 166–172. URL: <https://www.elibrary.ru/item.asp?id=43835845> (accessed: 05/15/2023).

3 ViPNet product line [Electronic resource]. Access mode: <https://infotecs.ru/product/> (accessed: 02/26/2023).

4 Chefranova A.O. Technology of building VPN ViPNet: a course of lectures: A textbook. Moscow: Prometheus, 2009. 180 p.