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[1], И. А. Базарова[2]

[1] ООО «Газинформсервис», г. Ухта;
[2]Ухтинский государственный технический университет, г. Ухта

P. S. Dvoretskaya[1], I. A. Bazarova[2]

[1]Gazinformservice LLC in Ukhta
[2]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 сеть 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).

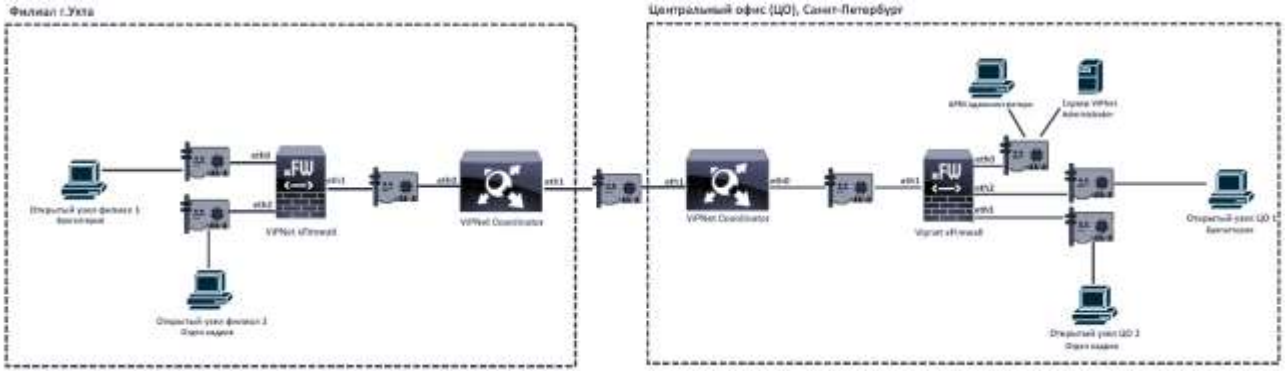

Рисунок 1. Схема макетируемой сети. Физический уровень

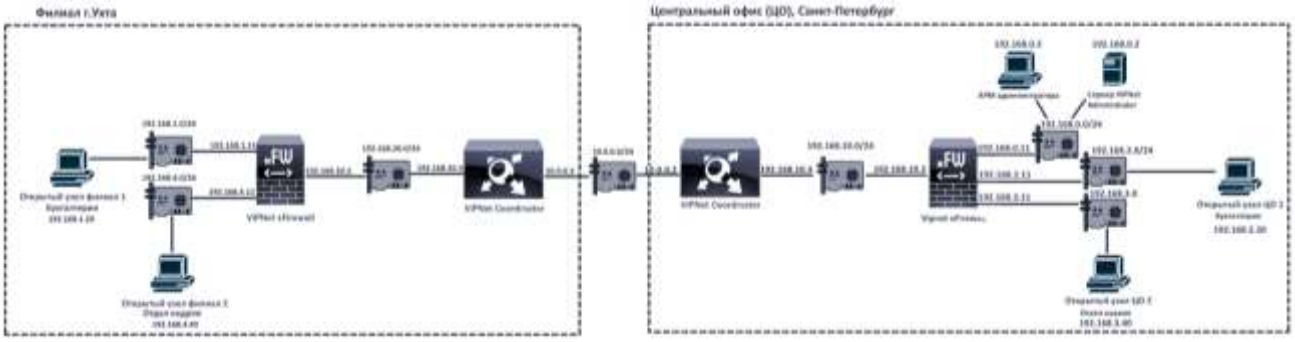

Рисунок 2. Схема макетируемой сети. Сетевой уровень

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

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, удается 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.

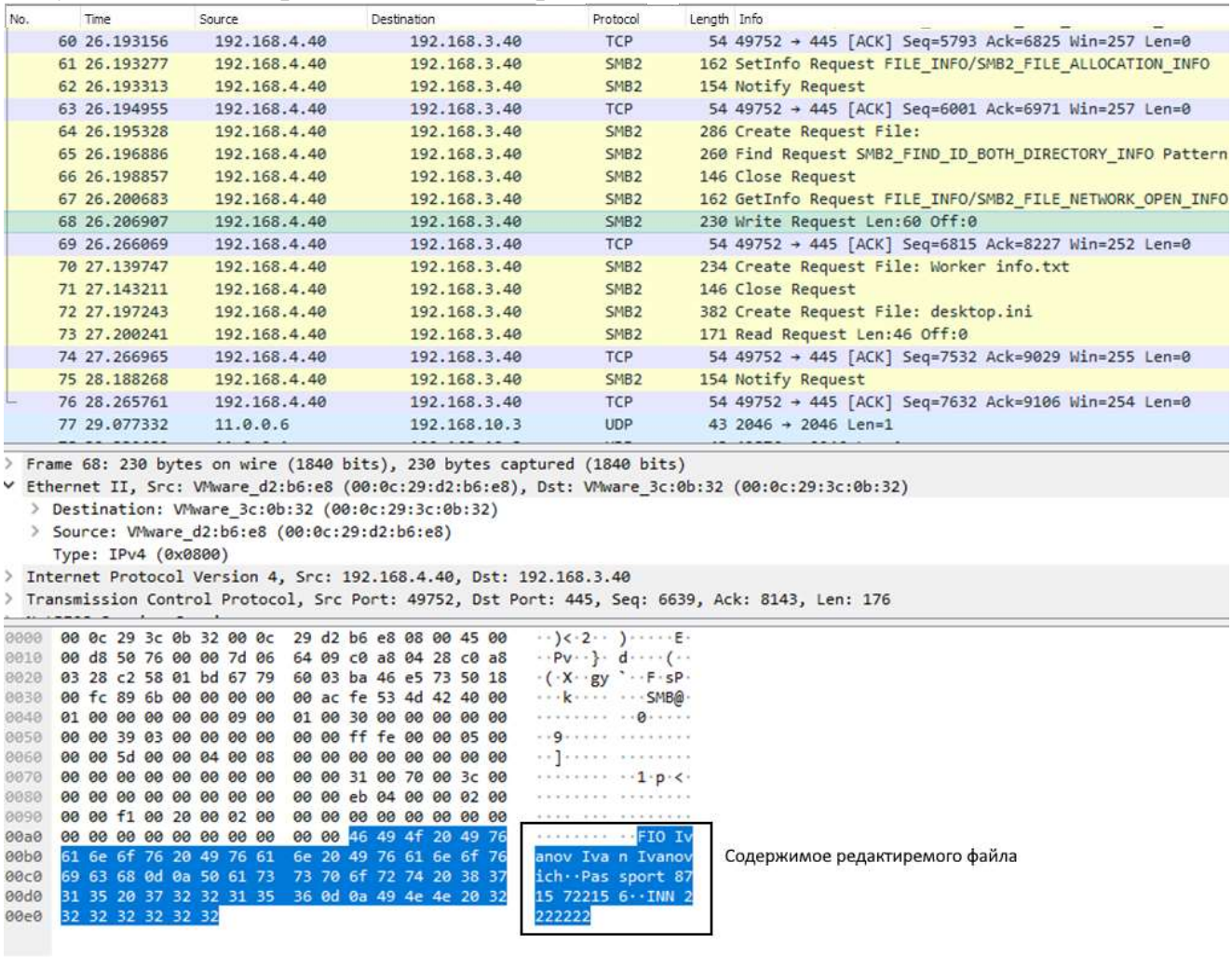

Рисунок 3. Открытый трафик, снятый с внутреннего интерфейса

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.

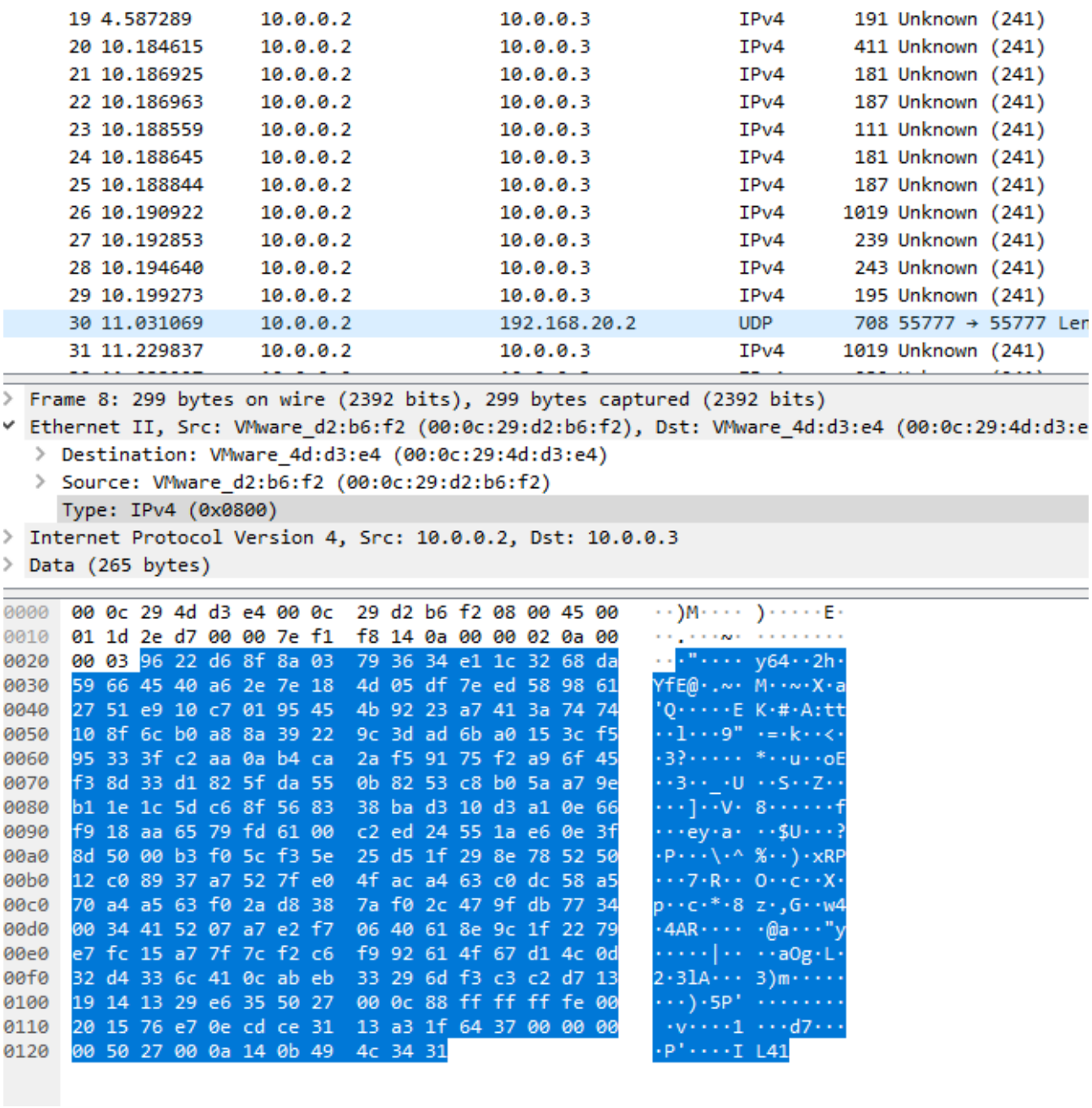

Рисунок 4. Зашифрованный трафик, снятый с внешнего интерфейса

Заключение

В данной статье дано кратное 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.