



Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Московский государственный технический университет  
имени Н.Э. Баумана  
(национальный исследовательский университет)»  
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)  
КАФЕДРА «Информационная безопасность» (ИУ8)

## ОТЧЁТ ПО УЧЕБНОЙ ПРАКТИКЕ

Тип практики: производственная практика

Название предприятия: ФГАУ «ФНФРО»

Студент:

Веденеев Максим Геннадьевич, группа ИУ8-62  
(3 курс)

Руководитель от предприятия:


Начальник отдела Васильев Владлен Николаевич

Руководитель от кафедры:

доцент кафедры ИУ8 Зайцева Анастасия Владленовна

Оценка: Отлично

 01.08.21  
(подпись, дата)

 01.08.21  
(подпись, дата)

\_\_\_\_\_  
(подпись, дата)



Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Московский государственный технический университет  
имени Н.Э. Баумана  
(национальный исследовательский университет)»  
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)  
КАФЕДРА «Информационная безопасность» (ИУ8)

## **ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ**

Тип практики: производственная практика

Название предприятия: ФГАУ «ФНФРО»

Сроки практики: с 19 июля 2021 г. по 01 августа 2021 г.

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»

**Задачами** производственной практики являются:

- Изучение методы контроля ЗИ на предприятии.
- Изучение технических и программных средств ЗИ на предприятии.
- Изучение систем защиты каналов связи на предприятии.
- Обеспечение защищенного соединения между филиалами компании.

Студент:

Веденеев Максим Геннадьевич, группа ИУ8-62

(3 курс)

Руководитель от предприятия:

Начальник отдела Васильев Владлен Николаевич

Руководитель от кафедры:

доцент кафедры ИУ8 Зайцева Анастасия Владленовна

 01.08.21  
(подпись, дата)

 01.08.21  
(подпись, дата)

\_\_\_\_\_  
(подпись, дата)

Является обязательным листом отчёта по практике. Лист 2

Документ не должен содержать информацию, отнесённую в установленном порядке к государственной тайне РФ.

## Оглавление

Перечень сокращений .....	4
Введение .....	5
Основная часть.....	7
1. Характеристика организации.....	7
2. Практическая часть.....	8
2.1 Методы контроля ЗИ на предприятии .....	8
2.2 Технические и программные средства ЗИ на предприятии .....	9
2.3 Системы защиты каналов связи на предприятии .....	<b>Ошибка! Закладка не определена.</b> 0
Заключение.....	17
Список использованных источников .....	18

## Перечень сокращений

- Firewall — функционал межсетевого экрана;
- IPSec VPN — построение частных виртуальных сетей;
- Mobile Access — удаленный доступ с мобильных устройств;
- IPS — система предотвращения вторжений;
- Anti-Bot — защита от ботнет сетей;
- AntiVirus — потоковый антивирус;
- AntiSpam & Email Security — защита корпоративной почты;
- Identity Awareness — интеграция со службой Active Directory;
- Monitoring — мониторинг практически всех параметров шлюза (load, bandwidth, VPN статус и т.д.)
- Application Control — межсетевой экран уровня приложений (функционал NGFW);
- URL Filtering — безопасность Web (+функционал проху);
- Data Loss Prevention — защита от утечек информации (DLP);
- Threat Emulation — технология песочниц (SandBox);
- Threat Extraction — технология очистки файлов;
- QoS — приоритезация трафика.



## **Введение**

### **Целью данной работы является:**

- приобретение профессионального опыта;
- овладение производственными навыками, необходимыми в экспериментально-исследовательской, проектной, организационно-управленческой и эксплуатационной деятельности;
- проверка готовности будущих специалистов к самостоятельной трудовой деятельности.

Основными задачами отдела защиты информации являются:

- разработка единой политики (концепции) обеспечения информационной безопасности организации, определение требований к системе защиты информации организации и документообороту на бумажных и электронных носителях;
- организация мероприятий и координация работ всех подразделений организации по комплексной защите информации на всех этапах технологических циклов ее создания, переноса на носитель (бумажный или электронный), обработки и передачи в соответствии с единой политикой обеспечения информационной безопасности организации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

Основными функциями отдела защиты информации являются:

- организация и координация действий подразделений организации по вопросам обеспечения информационной безопасности;
- экспертиза договоров организации со сторонними организациями по вопросам ОБИ при передаче (приеме) информации;
- участие в работе технической комиссии по пересмотру Перечня сведений, подлежащих защите
- согласование технических порядков по технологиям, связанным с информационным обменом и документооборотом;

- участие в проектировании, приемке, сдаче в промышленную эксплуатацию программных средств и АС организации (в части требований к средствам защиты информации);
- контроль за соблюдением правил безопасной эксплуатации АС организации;
- контроль за соблюдением требований ТУ и сертификатов на приобретенные программные и аппаратные средства (в том числе средства защиты информации);
- организация и контроль за разрешительной системой допуска исполнителей к работе с защищаемой информацией;
- определение порядка учета, хранения и обращения с защищаемой информацией (документами и носителями информации);
- контроль за сохранностью конфиденциальных документов и носителей информации;
- генерация ключей шифрования и ЭЦП.

## **Основная часть**

### **1. Характеристика организации**

Фонд новых форм развития образования (ФНФРО) обеспечивает организационную, методическую и информационную поддержку проектов по разработке и внедрению уникальных образовательных методик и педагогических инициатив.

Фонд содействует продвижению приоритетных направлений в образовании, стремится выявлять юные таланты, развивать интеллектуальные и творческие способности детей и молодёжи, а также обеспечивает их адаптацию к жизни в обществе и профориентацию.

Фонд является проектным офисом национального проекта «Образование» федеральным оператором сети детских технопарков «Кванториум», реализует масштабный пилотный проект по повышению доступности образования в России, разрабатывает уникальные образовательные методики.

В числе задач ФНФРО – организация мероприятий, информирующих общественность о передовых практиках в вопросах образования и воспитания.

## **2. Практическая часть**

### **1. Методы контроля ЗИ на предприятии**

Эффективное обеспечение защиты информации возможно только на основе комплексного использования всех известных методов и подходов к решению данной проблемы.

К концепции комплексной защиты предъявляется ряд требований:

- разработка и доведение до уровня регулярного использования всех необходимых механизмов гарантированного обеспечения требуемого уровня защищенности информации;
- существование механизмов практической реализации требуемого уровня защищенности;
- наличие средств рациональной реализации всех необходимых мероприятий по защите информации на базе достигнутого уровня развития науки и техники;
- разработка способов оптимальной организации и обеспечения проведения всех мероприятий по защите в процессе обработки информации.

Функции защиты информации:

- предупреждение возникновения условий, благоприятствующих появлению дестабилизирующих факторов;
- предупреждение непосредственного проявления дестабилизирующих факторов;
- обнаружение проявившихся дестабилизирующих факторов;
- предупреждение воздействия на защищаемую информацию проявившихся дестабилизирующих факторов;
- обнаружение воздействия дестабилизирующих факторов;
- локализация воздействия дестабилизирующих факторов;
- ликвидация последствий локализованного воздействия дестабилизирующих факторов.

Методики контроля ЗИ, используемые на предприятии:

- введение избыточности элементов системы;



- резервирование элементов системы;
- регулирование доступа к элементам системы;
- регулирование использования элементов системы;
- контроль элементов системы;
- маскировка информации;
- уничтожение информации;
- регистрация сведений.

## 2. Технические и программные средства ЗИ на предприятии

Рассмотрим основные средства, используемые для создания механизмов защиты.

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические.

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Из наиболее известных аппаратных средств можно отметить схемы контроля информации по четности, схемы защиты полей памяти — по ключу и т. п.

Физические средства реализуются в виде автономных устройств и систем. Это могут быть, например замки на дверях помещений, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Аппаратные средства, имеющиеся на предприятии:

- устройства для видеонаблюдения

- устройства для воспрепятствования несанкционированного включения рабочих станций и серверов:

- устройства уничтожения информации на магнитных и бумажных носителях:

- устройства сигнализации о попытках несанкционированных действий пользователей:

- устройства идентификации (распознавания) и аутентификации (проверки подлинности) субъектов (пользователей, процессов)

- устройства разграничение доступа к ресурсам

Программные средства, имеющиеся на предприятии:

- ПО для шифрования информации
- ПО для контроля и фильтрации трафика
- ПО для уничтожения информации
- ПО для идентификации (распознавания) и аутентификации (проверки подлинности) субъектов (пользователей, процессов)

- ПО для разграничения доступа к ресурсам
- ПО для обнаружения вредоносных программ
- ПО для тестового контроля
- ПО для резервного копирования информации
- DLP – системы
- SIEM – системы

### **3. Системы защиты каналов связи на предприятии**

В условиях нарастающих интеграционных процессов и создания единого информационного пространства проводятся работы по созданию защищенной телекоммуникационной инфраструктуры, связывающей удаленные офисы фирм в единое целое, а также обеспечение высокого уровня безопасности

информационных потоков между ними.

Применяемая технология виртуальных частных сетей позволяет объединять территориально распределенные сети как с помощью защищенных выделенных каналов, так и виртуальных каналов, проходящих через глобальные общедоступные сети. Последовательный и системный подход к построению защищенных сетей предполагает не только защиту внешних каналов связи, но и эффективную защиту внутренних сетей путем выделения замкнутых внутренних контуров VPN. Таким образом, применение технологии VPN позволяет организовать безопасный доступ пользователей в Интернет, защитить серверные платформы и решить задачу сегментирования сети в соответствии с организационной структурой.

Защита информации при передаче между виртуальными подсетями реализуется на алгоритмах асимметричных ключей и электронной подписи, защищающей информацию от подделки. Фактически данные, подлежащие межсегментной передаче, кодируются на выходе из одной сети, и декодируются на входе другой сети, при этом алгоритм управления ключами обеспечивает их защищенное распределение между оконечными устройствами. Все манипуляции с данными прозрачны для работающих в сети приложений.

При межсетевом взаимодействии между территориально удаленными объектами компании возникает задача обеспечения безопасности информационного обмена между клиентами и серверами различных сетевых служб. Сходные проблемы имеют место и в беспроводных локальных сетях (Wireless Local Area Network, WLAN), а также при доступе удаленных абонентов к ресурсам корпоративной информационной системы. В качестве основной угрозы здесь рассматривается несанкционированное подключение к каналам связи и осуществление перехвата (прослушивания) информации и модификация (подмена) передаваемых по каналам данных (почтовые сообщения, файлы и т.п.).

Для защиты данных, передаваемых по указанным каналам связи, необходимо использовать соответствующие средства криптографической защиты. Криптопреобразования могут осуществляться как на прикладном уровне (или на уровнях между протоколами приложений и протоколом TCP/IP), так и на сетевом



(преобразование IP-пакетов).

В первом варианте шифрование информации, предназначенной для транспортировки по каналу связи через неконтролируемую территорию, должно осуществляться на узле-отправителе (рабочей станции - клиенте или сервере), а расшифровка - на узле-получателе. Этот вариант предполагает внесение существенных изменений в конфигурацию каждой взаимодействующей стороны (подключение средств криптографической защиты к прикладным программам или коммуникационной части операционной системы), что, как правило, требует больших затрат и установки соответствующих средств защиты на каждый узел локальной сети. К решениям данного варианта относятся протоколы SSL, S-HTTP, S/MIME, PGP/MIME, которые обеспечивают шифрование и цифровую подпись почтовых сообщений и сообщений, передаваемых с использованием протокола HTTP.

Второй вариант предполагает установку специальных средств, осуществляющих криптопреобразования в точках подключения локальных сетей и удаленных абонентов к каналам связи (сетям общего пользования), проходящим по неконтролируемой территории. При решении этой задачи необходимо обеспечить требуемый уровень криптографической защиты данных и минимально возможные дополнительные задержки при их передаче, так как эти средства туннелируют передаваемый трафик (добавляют новый IP-заголовок к туннелируемому пакету) и используют различные по стойкости алгоритмы шифрования. В связи с тем, что средства, обеспечивающие криптопреобразования на сетевом уровне полностью совместимы с любыми прикладными подсистемами, работающими в корпоративной информационной системе (являются «прозрачными» для приложений), то они наиболее часто и применяются. Поэтому, остановимся в дальнейшем на данных средствах защиты информации, передаваемой по каналам связи (в том числе и по сетям общего доступа, например, Internet). Необходимо учитывать, что если средства криптографической защиты информации планируются к применению в государственных структурах, то вопрос их выбора должен решаться в пользу сертифицированных в России продуктов.



Для реализации второго варианта и обеспечения конфиденциальности и достоверности информации, передаваемой между объектами компании по каналам связи, можно использовать сертифицированные криптографические шлюзы (VPN-шлюзы). Например, Континент-К, VIPNet TUNNEL, ЗАСТАВА-Офис компаний НИП «Информзащита», Инфотекс, Элвис+. Эти устройства обеспечивают шифрование передаваемых данных (IP-пакетов) в соответствии с ГОСТ 28147-89, а также скрывают структуру локальной сети, защищают от проникновения извне, осуществляют маршрутизацию трафика и имеют сертификаты Гостехкомиссии РФ и ФСБ (ФАПСИ).

Криптошлюзы позволяют осуществить защищенный доступ удаленных абонентов к ресурсам корпоративной информационной системы (рис. 1). Доступ производится с использованием специального программного обеспечения, которое устанавливается на компьютер пользователя (VPN-клиент) для осуществления защищенного взаимодействия удаленных и мобильных пользователей с криптошлюзом. Программное обеспечение криптошлюза (сервер доступа) проводит идентификацию и аутентификацию пользователя и осуществляет его связь с ресурсами защищаемой сети.

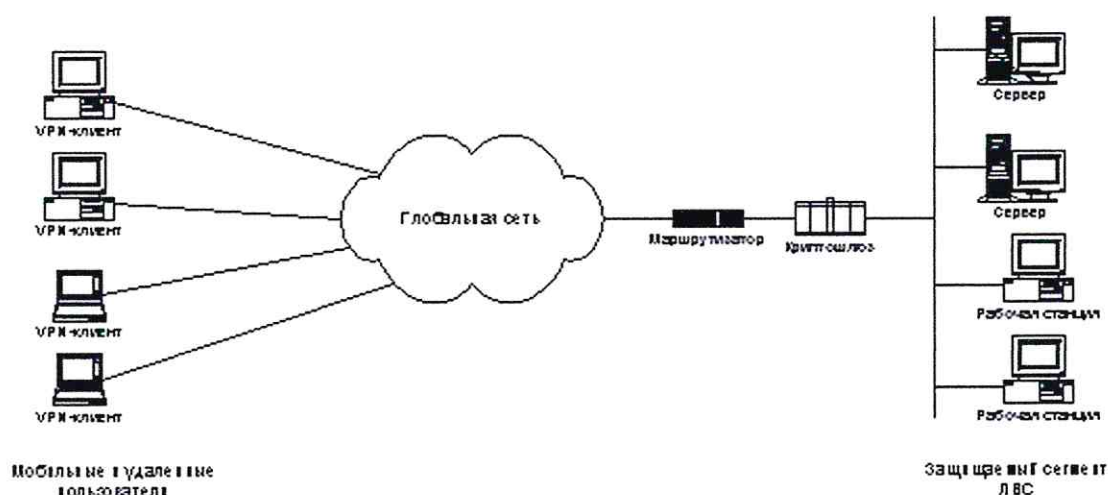


Рисунок 1 - «Удаленный доступ по защищенному каналу с использованием криптошлюза»

С помощью криптошлюзов можно формировать виртуальные защищенные

каналы в сетях общего пользования (например, Internet), гарантирующие конфиденциальность и достоверность информации и организовывать виртуальные частные сети (Virtual Private Network - VPN), которые представляют собой объединение локальных сетей или отдельных компьютеров, подключенных к сети общего пользования в единую защищенную виртуальную сеть. Для управления такой сетью обычно используется специальное программное обеспечение (центр управления), которое обеспечивает централизованное управление локальными политиками безопасности VPN-клиентов и криптошлюзов, рассылает для них ключевую информацию и новые конфигурационные данные, обеспечивает ведение системных журналов. Криптошлюзы могут поставляться как программные решения, так и как аппаратно-программные комплексы. К сожалению, большинство из сертифицированных криптошлюзов не поддерживает протокол IPSec и, поэтому они функционально не совместимы с аппаратно-программными продуктами других производителей.

Для начала разберемся, как это все работает. Итак, координатор ViPNet выполняет несколько функций. Во-первых, это криптошлюз (КШ), который позволяет реализовать как Site-to-site, так и RA VPN. Во-вторых, он является сервером-маршрутизатором конвертов, содержащих зашифрованные служебные данные (справочники и ключи) или данные клиентских приложений (файловый обмен, деловая почта). Кстати, именно в справочниках хранятся файлы, содержащие информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Координатор также является источником служебной информации для клиентов. Помимо этого, он может туннелировать трафик от компьютеров сети, где не установлен.

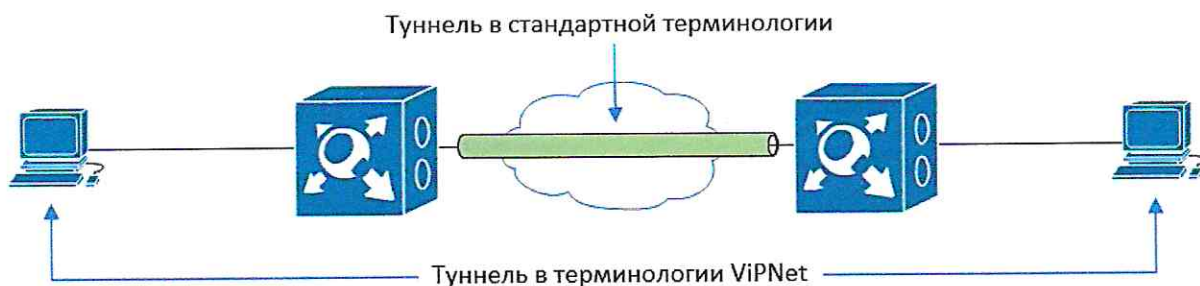


Рисунок 2 - Туннелирование.



В качестве протокола шифрования в ViPNet используется IP1ir, также разработанный «Инфотексом». Для инкапсуляции трафика применяются транспортные протоколы IP/241 (если трафик не покидает широковещательный домен), UDP/55777 и TCP/80. Для обеспечения полной безопасности корпоративной сети необходима установка программного обеспечения ViPNet, которое позволяет защитить не только корреспонденцию, передаваемую по сети, но и весь сетевой трафик, а также информацию, хранящуюся на компьютерах. При этом доступ к защищенному компьютеру с открытых или других защищенных компьютеров может быть в той или иной степени ограничен.

Для организации такой защиты необходимы следующие базовые элементы сети:

Рабочее место администратора ViPNet сети с установленным ПО:

ViPNet Administrator, состоящий из двух компонентов:

Центр управления сетью (ЦУС),

Удостоверяющий и ключевой центр (УКЦ);

ViPNet Client или ViPNet CryptoService для организации обмена служебной информацией с другими узлами сети ViPNet.

Сервер(ы) с установленным ПО ViPNet Coordinator, размещенный на границе сети или на границах участков сети. В зависимости от своей роли в сети координатор может выполнять различные функции.

Компьютеры пользователей с установленным клиентским ПО ViPNet Client или ViPNet CryptoService.

Помимо перечисленных базовых элементов, в сети ViPNet могут присутствовать и другие функциональные компоненты, решающие задачи резервирования, мониторинга, общего доступа к сертификатам и другие. Разновидности ПО ViPNet в зависимости от назначения и роли в сети представлены на схеме ниже.

Для подготовки рабочего места администратора сети ViPNet выполните следующие действия:

1. На сервере устанавливается ViPNet Coordinator и подключается к Интернету и локальным сетям
2. Установите на рабочем месте администратора ПО ViPNet Administrator. В случае необходимости установите компоненты ViPNet Administrator Центр управления сетью и ViPNet Administrator Удостоверяющий и ключевой центр на разные компьютеры.
3. В ЦУС создайте структуру защищенной сети ViPNet. В программе ViPNet Administrator ЦУС создаются сетевые узлы, указываются типы коллективов и создается логическая связь между ними, регистрация узлов в прикладных задачах
4. Создайте необходимое количество координаторов
5. На каждом координаторе зарегистрируйте необходимое количество абонентских пунктов.
6. Создайте межсерверные каналы для связи координаторов между собой.
7. Задать IP-адреса координаторов, туннелируемых узлов и настройки подключения координатора к сети в ЦУС во время регистрации сетевых узлов в прикладных задачах
8. Задайте правила трансляции адресов
9. В УКЦ сформируйте дистрибутив ключевой информации
10. Формируются справочники и создаются дистрибутивы ключей
11. На абонентском пункте следует установить один из двух компонентов ПО ViPNet:

ViPNet Client — выполняет функции VPN-клиента сети ViPNet и персонального сетевого экрана.

ViPNet CryptoService — обеспечивает возможность использования криптографических функций в прикладных программах, но не обеспечивает защиту трафика.

12. Настройте параметры межсетевого экрана

Задайте IP-адрес сервера IP-адресов, выбранного для данного абонентского пункта



Настройте интегрированный сетевой экран:

Настройте параметры обработки прикладных протоколов и веб-фильтры

13. Чтобы убедиться в том, что сеть ViPNet развернута и настроена правильно, достаточно проверить возможность установления соединений между сетевыми узлами ViPNet.

14. Для проверки соединения с выбранными сетевыми узлами в программе ViPNet Монитор нажмите кнопку Проверить соединение

15. Для проверки соединения с туннелируемыми узлами можно воспользоваться командой ping.

Для полноценного функционирования сети необходима возможность соединения между всеми координаторами, а также между абонентскими пунктами и их серверами IP- адресов.

После успешного прохождения проверки локальной работоспособности, нужно провести аналогичные действия на других местах, где предполагается использование ViPNet.

## **Заключение**

Знания, умения, навыки, полученные за период прохождения практики, явились отличным стимулом для активной работы в освоении будущей специальности, позволили практически реализовать теоретически изученные моменты, получить первый профессиональный опыт работы и сформировать общее представление о специфике деятельности патентного информационного фонда.

Цель производственной практики, которая заключалась в изучении методов контроля ЗИ на предприятии, изучение работы технических и программных средств ЗИ на предприятии.

Изучение систем защиты каналов связи на предприятии.

Обеспечение защищенного соединения между филиалами компании.

В процессе прохождения были изучены информационные системы, меры и средства для их защиты, официальные документы предприятия, нормативная и методическая документация, которые позволили решить многие поставленные задачи. В ходе прохождения преддипломной практики я ознакомился с организационной структурой, рассмотрел информационную систему обработки персональных данных, построил для неё модель угроз и модель нарушителя, определил класс и тип и рассчитал актуальные угрозы ИСПДн. Также ознакомился с новыми программными средствами обеспечения безопасности информации. Осмотрел различное оборудование и получил краткую характеристику по каждому из них. В процессе прохождения практики я влился в рабочий коллектив, почувствовал весь рабочий процесс предприятия.

Немаловажным является тот факт, что в процессе прохождения практики были получены новые теоретические и практические знания в области информационной безопасности, которые несомненно будут использованы при написании дипломной работы:

Исходя из всего вышеизложенного, можно сделать выводы, что все поставленные на преддипломную практику цели и задачи были выполнены.

### Список использованных источников

- 1) Информационная безопасность: Защита и нападение [Текст] / А. Бирюков. 2-е изд. — ДМК Издательство, 2017. — 433 с.
- 2) Сравнение универсальных шлюзов безопасности. [Электронный ресурс]. — Режим доступа: <https://www.anti-malware.ru/compare/USG-NGFW> (Дата обращения: 28.07.2021).
- 3) Построение безопасных сетей на основе VPN. [ссылка]. [просмотрено 16.07.2021] <http://www.aitishnik.ru/seti/postroenie-bezopasnich-setey-na-osnove-vpn.html>