Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет информатики и радиоэлектроники»

ОТЧЁТ

О ПРОХОЖДЕНИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ НА ПРЕДПРИЯТИИ «НАЦИОНАЛЬНЫЙ ЦЕНТР ОБМЕНА ТРАФИКОМ»

Выполнила: Проверила:

Савченко Е.А. Бойправ О.В.

Минск 2022

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc105685565)

[1 ИЗУЧЕНИЕ ОРГАНИЗАЦИОННО-ПРАВОВОЙ СТРУКТУРЫ ПРЕДПРИЯТИЯ 4](#_Toc105685566)

[2 АНАЛИЗ СРЕДСТВ ТЕЛЕКОММУНИКАЦИЙ, ИСПОЛЬЗУЕМЫХ НА ПРЕДПРИЯТИИ 5](#_Toc105685567)

[1.1 Заголовок 5](#_Toc105685568)

[1.2 Заголовок 5](#_Toc105685569)

[3 АНАЛИЗ МЕТОДОВ И СРЕДСТВ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМЫХ НА ПРЕДПРИЯТИИ 6](#_Toc105685570)

[3.1 Заголовок 6](#_Toc105685571)

[3.2 Заголовок 6](#_Toc105685572)

[4 РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ МЕТОДОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМЫХ НА ПРЕДПРИЯТИИ 7](#_Toc105685573)

[4.1 Заголовок 7](#_Toc105685574)

[4.2 Заголовок 7](#_Toc105685575)

[ЗАКЛЮЧЕНИЕ 8](#_Toc105685576)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 9](#_Toc105685577)

# ВВЕДЕНИЕ

Производственная практика является одним из важнейших этапов подготовки специалистов. Целью производственной практики является закрепление и углубление практических знаний, полученных во время обучения, ознакомление с организационной структурой, производственными процессами и автоматизированными системами предприятия, приобретение профессиональных навыков, изучение информационных технологий, разрабатываемых и используемых на предприятии, приобретение навыков эксплуатации ИТ-систем и их компонентов.

Индивидуальное задание на время прохождения производственной практики состояло в следующем:

– изучение организационно-правовой структуры предприятия;

– изучение средств телекоммуникаций, используемых на предприятии;

– анализ методов и средств по защите информации, используемых на предприятии;

–разработка рекомендаций по улучшению методов по защите информации, используемых на предприятии.

Практика проходила на базе ГУП «Национальный центр обмена трафиком», было создано согласно Указу Президента Республики Беларусь от 30 сентября 2010 года № 515 «О некоторых мерах по развитию сети передачи данных в Республике Беларусь» в целях развития в Республике Беларусь современной инфраструктуры сети передачи данных на основе внедрения новых информационно-коммуникационных технологий, привлечения в эту сферу отечественных и иностранных инвестиций, повышения качества и снижения стоимости оказываемых услуг передачи данных.

НЦОТ осуществляет свою деятельность в соответствии с [лицензией № 02140/2183 на оказание услуг электросвязи](https://ncot.by/ru/about/license/), выданной Министерством связи и информатизации Республики Беларусь на основании решения № 2 от 17 января 2011 года. Предприятие было зарегистрировано за регистрационным номером 191435810 решением Минского горисполкома от 11 ноября 2010 года.

НЦОТ имеет право на присоединение к сетям электросвязи иностранных государств и пропуск международного трафика и право на осуществление деятельности по технической и (или) криптографической защите информации ([лицензия № 01019/421 от 28.02.2019 года](https://ncot.by/ru/about/license/)).

# 1 ИЗУЧЕНИЕ ОРГАНИЗАЦИОННО-ПРАВОВОЙ СТРУКТУРЫ ПРЕДПРИЯТИЯ

Во время прохождения производственной практики было выяснено, что руководит предприятием директор, имеющий двух непосредственных заместителей – первого заместителя директора и заместителя директора.

Первый заместитель директора курирует работу: управления по взаимодействию с операторами, отдела по расчетам, группы маркетинга, отдела образовательных услуг и группы управления проектами.

В подчинении заместителя директора находятся: управление эксплуатации сети, в составе которого находится группа оперативного контроля, управление информационной безопасности, отдел развития телефонной сети, отдел информационных технологий, отдел противодействия нарушениям пропуска трафика и административно-хозяйственный отдел.

Основными задачами предприятия являются:

– развитие в Республике Беларусь современной инфраструктуры сети передачи данных;

– внедрение новых информационно-коммуникационных технологий;  
– привлечение в эту сферу отечественных и иностранных инвестиций;  
– повышение качества, снижение стоимости оказываемых услуг передачи данных;

– развитие защищённого сегмента ЕРСПД с криптографической защитой.

Основные услуги, предоставляемые предприятием представлены на рисунке 1.1

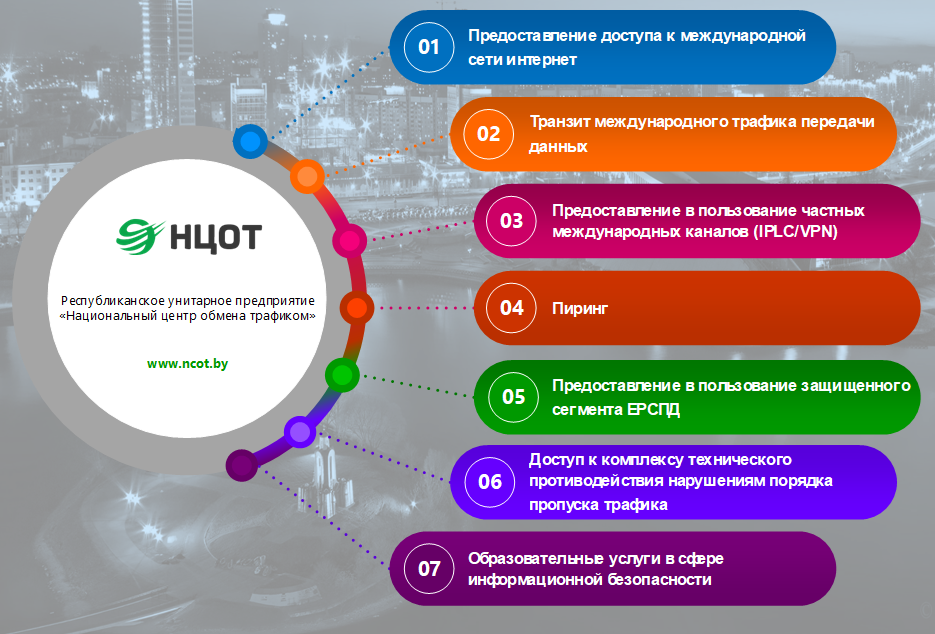


Рисунок 1.1 – Перечень предоставляемых услуг

# 2 АНАЛИЗ СРЕДСТВ ТЕЛЕКОММУНИКАЦИЙ, ИСПОЛЬЗУЕМЫХ НА ПРЕДПРИЯТИИ

На предприятии «НЦОТ» используется большое количество средств телекоммуникаций различных производителей: Cisco, Huawei, ProLiant, FortiGate и другие. В отчете для примера представлены выборочные модели оборудования.

## 2.1  Маршрутизатор Cisco C111-4P

Cisco C1111-4P – это современный высокопроизводительный беспроводной роутер, который входит в линейку оборудования Cisco 1100 Series Integrated Services Routers, которая ориентирована на филиалы, а также компании малого и среднего размера. Устройство имеет широкие функциональные возможности, и обеспечивает высокий уровень надёжности и сетевой безопасности. Маршрутизатор представлен на рисунке 2.1.1.



Рисунок 2.1.1 – Маршрутизатор CISCO C1111-4P

Технические характеристики маршрутизатора CISCO C1111-4 представлены в таблице 2.1.

Таблица 2.1.1 – Технические характеристики маршрутизатора CISCO.

|  |  |
| --- | --- |
| Параметр | Значение |
| Тип установки | Настольное |
| Универсальные порты Ethernet | 1 х SFP combo |
| WAN порты Ethernet | 1 x GE |
| LAN порты Ethernet | 4 x GE |
| Память FLASH | 4 Гб |
| Память FLASH максимум | 4 Гб |
| Объем ОЗУ | 4 Гб |
| Память ОЗУ максимум | 4 Гб |
| Потребляемая мощность | 12,5 Вт |
| Порты USB | 1 x USB 3.0 |
| Высота, мм | 42 |
| Размеры (В х Ш х Г), мм | 42 x 323 x 230 |

## 2.2 Коммутатор Cisco Catalyst 9200

Cisco Catalyst 9200 (C9200L-24T-4G-A) – это стекируемый сетевой коммутатор корпоративного класса, предоставляющий расширенные функции безопасности, которые защищают целостность аппаратного и программного обеспечения, а также всех данных, проходящих через коммутатор. Коммутатор представлен на рисунке 2.2.1.



Рисунок 2.2.1 – Коммутатор Cisco Catalyst 9200

Технические характеристики коммутатора Cisco Catalyst 9200 представлены в таблице 2.2.1.

Таблица 2.2.1 – Технические характеристики коммутатора CISCO.

|  |  |
| --- | --- |
| Параметр | Значение |
| Тип установки | Стоечное |
| Универсальные порты Ethernet | 24 x GE RJ-45 |
| WAN порты Ethernet | 4 х 1GE |
| LAN порты Ethernet | 24 x Ethernet 10/100/1000 |
| Память FLASH | 4 Гб |
| Память FLASH максимум | 4 Гб |
| Объем ОЗУ | 2 Гб |
| Память ОЗУ максимум | 2 Гб |
| Потребляемая мощность | 12,5 Вт |
| Порты USB | 2 x USB 3.0 |
| Высота, мм | 444 |
| Размеры **(**Вх Ш х Г), мм | 444x44x288 |
| Тип питания | АС 100-240В |

## 2.3  Сервер ProLiant DL180 Gen10

ProLiant DL180 Gen10 P35519-B21 – безопасный современный сервер. Отличается масштабируемостью, производительностью и надежностью, что делает его идеальной платформой для компаний, готовых к использованию локальных и гибридных облачных приложений. Таким компаниям требуется оптимальное сочетание вычислительных ресурсов и систем хранения данных для достижения важнейших целей. Сервер изображен на рисунке 2.3.1



Рисунок 2.3.1 – Сервер ProLiant DL180 Gen10 P35519-B21

Основные технические характеристики сервера занесены в таблицу 2.2.3

Таблица 2.3.1 – Технические характеристики сервера.

|  |  |
| --- | --- |
| Параметры | Значение |
| Процессор | Intel Xeon Silver 4210R 2,4ГГц |
| Тактовая частота процессора | 2400МГц |
| Количество разъемов | 2x1Gb Ethernet |
| Объем оперативной памяти | 16 Гб |
| Тип памяти | DDR4-2933 Registered |
| Мощность | 500 Вт |
| Тип шасси | SFF Easy Install Rail Kit |
| Контроллер | 2 x 1Gbe (HPE Ethernet 332i) |
| Размеры (В х Ш х Г), см | 46×60×19 |

## 2.4 Межсетевой экран FortiGate-60E

Межсетевые экраны серии FortiGate-60E обеспечивают превосходный уровень сетевой безопасности в компактном форм-факторе. Решение FortiGate-60E идеально подходит для малых и средних офисов и филиалов.

Все устройства FortiGate построены на уникальных FortiASIC System on a Chip 3 (SoC3), что обеспечивает полный набор всех функций для защиты приложений и данных.Защита от эксплойтов, вредоносных программ и сайтов обеспечивается с помощью FortiGuard Labs. Определение и анализ типов возникающих угроз позволяет эффективно бороться с таргетированными атаками.

Возможности объединения в одном устройстве не только функций безопасности, а также маршрутизации, коммутации, контроллера беспроводных сетей и производительного Ipsec VPN обеспечивают широкие возможности применения FortiGate в корпоративном сегменте.



Рисунок 2.4.1 – Межсетевой экран FortiGate-60E

Основные технические характеристики межсетевого экрана занесены в таблицу 2.4.1

Таблица 2.4.1 – Технические характеристики межсетевого экрана.

|  |  |
| --- | --- |
| Параметры | Значение |
| Применение | для сетей Ethernet |
| Количество WAN портов | 2 |
| Количество LAN портов | 7 |
| Тип LAN портов | 10/100/1000T BaseTx |
| MPN | FG-60E |

# 3 АНАЛИЗ МЕТОДОВ И СРЕДСТВ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМЫХ НА ПРЕДПРИЯТИИ

## 3.1 Межсетевые экраны

В соответствии с политикой реализации межсетевых экранов определяются правила доступа к ресурсам внутренней сети. Прежде всего установлено насколько «доверительной» или «подозрительной» должна быть система защиты. Иными словами, правила доступа к внутренним ресурсам базируются на следующих принципов:

– Запрещать все, что не разрешено в явной форме

– Разрешать все, что не запрещено в явной форме.

Эффективность защиты внутренней сети с помощью межсетевых экранов зависит не только от выбранной политики доступа к сетевым сервисам и ресурсам внутренней сети, но и от рациональности выбора и использования основных компонентов межсетевого экрана.

На предприятии «НЦОТ» используется девять межсетевых экранов, восемь из которых PFSense и один – fortigate 60e.

Могу сделать вывод, что pfSense в абсолютном большинстве случаев вполне способен служить заменой коммерческим решениям от той же Cisco. Если при этом добавить возможность добавления пакетов из репозитория самого pfSense, то он даже в чем-то их и превосходит. Но нужно четко осознавать: pfSense заточен под типичные конфигурации. Да, кирпичиков этих самых типичных конфигураций в нем много, однако стоит от них отступить, и окажется, что сделать нечто нестандартное в pfSense не представляется возможным.

Таким образом, если конфигурация сети крайне неординарна, лучше использовать коммерческие решения или пилить роутер самостоятельно на основе той же Free/OpenBSD/Linux. В противном же случае, pfSense выглядит не худшим вариантом.

Межсетевой экран fortigate 60e является экраном следующего поколения (NGFW). Он фильтрует сетевой трафик для защиты организации от внутренних и внешних угроз. Наряду с поддержкой функций межсетевых экранов с проверкой состояния, таких как фильтрация пакетов, поддержка IPsec и SSL VPN, мониторинг сети и функции сопоставления IP-адресов, решения NGFW включают возможности более глубокой проверки содержимого. Эти возможности позволяют выявлять атаки, вредоносное ПО и другие угрозы, а также позволяют межсетевым экранам NGFW блокировать эти угрозы. Решения NGFW предоставляют организации возможности проверки SSL, контроля приложений, предотвращения вторжений и расширенные функции отслеживания всей поверхности атаки.

## 3.2 SIEM-система

Системы защиты, известные под аббревиатурой SIEM, появились в результате эволюции и слияния SEM и SIM.

SEM – Security Event Management – система защиты, которая работает в режиме реального времени. Она самостоятельно наблюдает за событиями в информационных потоках, собирает их, производит корреляцию и генерирует превентивные сообщения.

SIM – Security Information Management – система, которая отвечает за анализ сведений на основе статистики и девиаций от установленных правил безопасности.

На предприятии «НЦОТ» используется система мониторинга и корреляции событий информационной безопасности – LibraSIEM.

Такая система в режиме реального времени осуществляет сбор и анализ событий безопасности, выявляя инциденты и предоставляя ИБ-специалисту всю необходимую информацию для принятия решения.

LibraSIEM находит потенциально опасные действия пользователей или администраторов, критические события в средах защиты, попытки несанкционированного доступа к информации, неполадки в корпоративных системах, аппаратные и программные сбои.

На рисунке 3.2.1 представлена схема работы данной системы.



Рисунок 3.2.1 – Схема работы LibraSIEM

Как видно из рисунка, система работаем поэтапно:

– собирает логи из различных источников;

– анализирует сведения, согласно настройкам(политикам безопасности);

–обнаруживает инциденты и сообщает об этом специалисту по безопасности

К преимуществам данной системы относятся:

– простое внедрение;

– простая эксплуатация;

– простая интеграция с IT-инфраструктурой и другими ИБ-решениями;

– простые технические требования

## 3.3 Корпоративная почта

В качестве способа защиты информации передаваемой через корпоративную почту используется облачное хранилище, точнее услуга «корпоративная почта», предоставляемая компанией becloud.

Такой сервис реализован на базе корпоративной платформы Microsoft Exchange Server, является защищенным и подходит для использования в том числе государственными органами и организациями.

## Возможности услуги «Корпоративная почта»:

* Подключение любого количества почтовых ящиков объемом от 2ГБ. При необходимости объем ящика увеличивается по запросу.
* Назначение корпоративного адреса электронной почты. При необходимости для одного ящика можно назначить несколько адресов электронной почты.
* Управление электронной почтой, календарями, задачами через веб-интерфейс, настольную или мобильную версию Outlook.
* Синхронизация с рабочим компьютером, планшетом и любым другим мобильным устройством.
* Возможность сортировки почты, назначения приоритетов важным сообщениям, персонализация настроек исходя их своих предпочтений.
* Планирование собраний и папки общего доступа.
* Резервное копирование ящиков.

## beCloud предлагает:

* Надежное хранение данных, безопасную передачу сообщений по SSL-протоколу.
* Защиту почтового трафика сертифицированными решениями компании «Лаборатория Касперского».
* Гарантии работоспособности услуги с уровнем доступности 99,5%.
* Надежную защиту информации на уровне республиканской платформы, соответствующей требованиям законодательства Республики Беларусь.

## 3.4 Удаленный доступ

Для осуществления удаленного доступа на предприятии «НЦОТ» используются устройства аппаратно-программного ip шифрования для обработки информации ограниченного распространения «река» и «река-м».

Устройство аппаратно-программное IP шифрования "РЕКА-M" (IP-шифратор) предназначено для криптографической защиты информационного обмена между локальными сетями и/или отдельными станциями, взаимодействующими по протоколу IP через сети передачи данных. Программное обеспечение IP-шифратора «Река-М» устанавливается на ПЭВМ (либо портативный компьютер или планшет) потребителя с операционной системой типа Windows 7 SP1, Windows 8.1, Windows 10.

Обеспечивает:

• криптографическую защиту IP-пакетов методом полной инкапсуляции (протокол IPsec Encapsulating Security Payload);

• прозрачное автоматическое шифрование/расшифрование информации с заданной стойкостью по алгоритму шифрования ГОСТ 28147-89, СТБ 34.101.31-2011, AES256; • агрегированную скорость шифрования (зависит от производительности центрального процессора аппаратной платформы) около 100 Мбит/с; • контроль целостности пакетов данных – имитозащиту по ГОСТ 28147-89 или СТБ 34.101.31-2011, SHA256;

•ключевую систему – полносвязную ключевую матрицу с индивидуальными ключами на каждом направлении обмена; • работу в сети до 1000 изделий (одновременное функционирование по 1 (одному) виртуальному каналу); • доступ к программе управления IP-шифратора через средство криптографической защиты (СКЗИ) «Сигма»; • круглосуточную необслуживаемую работу.

Для генерации ключа, предназначенного для шифрования ключей, загружаемых в изделие с внешних носителей, хэш-значений паролей пользователей, используется датчик случайных чисел СКЗИ «Сигма». Хранение, обновление и уничтожение ключа безопасности производится средствами СКЗИ «Сигма».

IР-шифратор эксплуатируется на ПЭВМ потребителя со следующими характеристиками:

• операционная система (ОС) Windows 7 SP1 (с установленным пакетом обновления KB3033929), Windows 8.1, Windows 10;

• объем накопителя на жестком магнитном диске – не менее 40 Гб;

• объем оперативной памяти – не менее 1 Гб;

• тактовая частота процессора – не менее 2 ГГц.

Устройство аппаратно-программное IP шифрования "РЕКА" (IP-шифратор) предназначено для криптографической защиты информационного обмена между локальными сетями и/или отдельными рабочими станциями, взаимодействующими по протоколу IP через сеть передачи данных.

**IP-шифратор обеспечивает:**  
- подключение по стыкам Ethernet стандарта IEEE 802.3 (100 Мбит/с) к защищаемой ЛВС и сетевому оборудованию транспортной сети по медным или оптическим кабелям;  
- криптографическую защиту IP-пакетов методом полной инкапсуляции;  
- прозрачное автоматическое шифрование/расшифрование информации с заданной стойкостью по алгоритму шифрования ГОСТ 28147-89 или СТБ 34.101.31-2011, с возможностью замены алгоритма (АЕS256);  
- контроль целостности пакетов данных - имитозащиту по ГОСТ 28147-89 или СТБ 34.101.31-2011, с возможностью замены алгоритма (НМАС);  
- генерацию ключей для работы в сети с использованием датчика случайных чисел на основе физического источника шума;  
- одновременную работу в сети до 1000 изделий (обеспечение одновременного функционирования до 1000 виртуальных каналов);  
- защиту от несанкционированного доступа при вскрытии корпуса;  
-  ведение автономного журнала аудита;  
-  круглосуточную необслуживаемую работу;  
-  мониторинг работы изделия на ПЭВМ, подключаемой к портам изделия.

# 4 РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ МЕТОДОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМЫХ НА ПРЕДПРИЯТИИ

## 4.1 Заголовок

Текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст.

## 4.2 Заголовок

Текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст.

# ЗАКЛЮЧЕНИЕ

Текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. https://www.fortinet.com/ru/products/next-generation-firewall

2. https://www.ncot.by/ru/about/about/

https://librasoft.by/LibraSIEM\_rus\_web.pdf

https://becloud.by/services/uslugi-rtsod/po-kak-usluga-saas/korporativnaya-pochta/?action=change\_lang&\_ga=2.32734525.2091289954.1656444970-439009273.1656444970

http://niitzi.by/images/Buklet/2020/NII%20TZI%20rus.pdf

https://www.bvpservice.by/catalog/sredstva-svyazi-i-sredstva-zaschity-informacii/ustroystvo-apparatno-programmnoe-ip