МИНИСТЕРСТВО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
И ЗАНЯТОСТИ НАСЕЛЕНИЯ ПРИМОРСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ДАЛЬНЕВОСТОЧНЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

ОТЧЕТ
производственной (по профилю специальности) практики

Специальность: 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

(код *и название специальности)*

ПМ 03 «Защита информации техническими средствами»

(Код, наименование ПМ)

Обучающийся Шаркунов Кирилл Алексеевич
(Ф.И.О.)

4 курса 842 группы

Проходившего (шей) практику с __13_ марта_____ по _10 апреля___ 2023 г.

Место прохождения практики: _Акционерное общество «Мегафон-Ритейл», Приморский край, город Уссурийск, Ленина 62_____
_____
__

Руководитель практики от предприятия: ____Бородинов Владимир Вячеславович, Менеджер _____
_____
__
(Ф.И.О. полностью, должность)

_10__апреля___2023 г. _____
(дата) (подпись)

г. Уссурийск

2023г.

Оглавление

Введение

Формирование у обучающихся практических профессиональных умений в рамках профессионального модуля по основному виду профессиональной деятельности «Применение инженерно-технических средств обеспечения информационной безопасности», необходимых для последующего освоения ими общих и профессиональных компетенций, предусмотренных ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

С целью комплексного освоения профессиональной деятельности студент должен по виду профессиональной деятельности «Защита информации техническими средствами»:

иметь практический опыт:

- выявления технических каналов утечки информации;
- использования основных методов и средств инженерно-технической защиты информации;
- диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;
- участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;
- решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;

уметь:

- применять технические средства защиты информации;
- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
- использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам; - применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами;

знать:

- физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;
- основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам;

- номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

Преддипломная практика направлена на углубление первоначального практического опыта обучающегося, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы в организациях различных организационно-правовых форм.

В рамках реализации сформулированной цели, основные задачи преддипломной практики определены следующим образом:

- закрепление и совершенствование приобретенного в процессе обучения опыта практической деятельности обучающихся в сфере получаемой специальности;
- развитие общих и профессиональных компетенций;
- приобретение студентами навыков организаторской работы и оперативного управления производственным участком при выполнении обязанности дублеров инженерно-технических работников со средним профессиональным образованием; ознакомление непосредственно на производстве с передовой технологией, организацией труда и экономикой производства; развитие профессионального мышления и организаторских способностей в условиях трудового коллектива;
- адаптация обучающихся к конкретным условиям деятельности предприятий различных организационно-правовых форм, органов государственной власти и местного самоуправления;
- подготовка к выполнению выпускной квалификационной работы в организациях различных организационно-правовых форм, органах государственной власти и местного самоуправления

Тема 1. Аппаратно-программный комплекс организации

Обмен данными различных типов внутри организации осуществляется в форме потоков информации. Учитывая масштабы предприятия, необходимо организовать максимально оптимизированное и рациональное перемещение информационных потоков в системе. Оперативность выполнения каждым отделом, возложенных на него функций, а значит и эффективность

деятельности организации в целом, напрямую зависит от правильно налаженной работы систем регистрации, передачи, хранения и обработки информации.

Служба безопасности взаимодействует со всеми отделами организации, не имея при этом обратных информационных потоков, что объясняется спецификой работы данного подразделения. В первую очередь осуществляется сбор, анализ и регулирование доступа к данным, подлежащим защите. В этом направлении особое внимание следует обратить на связи со следующими отделами:

отдел администрирования и коммутации информационных потоков, основное направление - работа с системами скремблирования полезного трафика в сети GSM; контроль разграничения доступа к различным уровням системы;

отдел биллинговых систем - контроль доступа к персональным данным клиентов (база данных подписчиков услуг оператора); контроль над транзакциями внутри системы биллинга (анализ операций внесения и списания денежных средств);

отдел бухгалтерского учета и аудита - работа с информацией о финансовой стороне деятельности организации; анализ результатов аудита деятельности предприятия;

отдел кадров - проверка сведений, предоставляемых вновь прибывшими сотрудниками; разграничение прав доступа персонала на различных уровнях функционирования организации.

Кроме того, взаимодействие данного подразделения со всеми отделами организации предполагает контроль состояния и обеспечение функционирования защиты информационной системы предприятия; особое внимание уделяется организации защиты информации, относящейся к коммерческой тайне и к персональным данным; сбор и анализ отчетов обо всех возникших инцидентах безопасности, для принятия соответствующих мер, в случае необходимости.

Административный отдел организации поддерживает двусторонний обмен информационными потоками с каждым направлением предприятия, для выполнения своих прямых функций по координированию работы между направлениями в составе единой инфраструктуры. Передаваемые данные, в своем большинстве носят характер директив, протоколов и отчетов о проведенных мероприятиях и возникших внештатных ситуациях, работа с персональными данными в данном случае сведена к минимуму. Наиболее плотное взаимодействие осуществляется с отделом планирования и отделом маркетинга и рекламы.

Дополнительно, осуществляется обмен данными с управляющим аппаратом организации, в лице исполнительного директора по области или его заместителя. По запросу, административный отдел передает информацию о своей деятельности или деятельности других отделов, в форме отчетов, службе безопасности, о чем было упомянуто ранее.

Отдел администрирования и коммутации информационных потоков обрабатывает и генерирует два типа данных по функциям:

статистическая информация - направляется в отдел мониторинга, представляет собой данные об объемах предоставленных клиентам организации сервисов, например длительность голосовых соединений, интенсивность использования сервисов коротких сообщений, и др.;

данные и команды управления - принимаются и обрабатываются из отдела биллинговых систем, являют собой информацию о состоянии персональных счетов абонентов, и, соответственно, разрешение на предоставление телекоммуникационного ресурса для оказания тех или иных услуг.

Дополнительно, подразделением осуществляется обмен информацией с административным отделом и службой безопасности организации. Характер передаваемых данных указан в описании информационных потоков соответствующих отделов.

Отдел биллинговых систем в результате своей основной деятельности задействует информационные потоки со следующими отделами:

отдел администрирования и коммутации информационных потоков - данные о состоянии персонального счета клиента;

отдел бухгалтерского учета и аудита - передаются данные о совокупных объемах вырученных и затраченных средств по предоставлению телекоммуникационных услуг.

Кроме вышеперечисленного, направлением ведется обмен данными со службой безопасности и административным отделом организации. Следует обратить внимание на то, что по роду деятельности данного отдела, может произойти раскрытие персональных данных подписчиков услуг оператора сотовой связи.

Отдел планирования предприятия с точки зрения обмена информацией, работает по двум основным направлениям: сбор разнородных специфических данных, образующихся в результате деятельности различных подразделений организации; и предоставление результатов собственной работы по каждой структурной единице оператора. Отделом осуществляется непосредственная связь с аппаратом управления организации. В этом случае передаваемая информация может быть отнесена к "коммерческой тайне", так как ей присущи все черты деловой информации организации.

Основной поток информации, необходимый для эффективной работы подразделения, поступает из отдела мониторинга. Данные носят исключительно статистический характер, без привязки к персональному идентификатору абонента, и, следовательно, его персональным данным. При этом сохраняются все упомянутые ранее связи.

Отдел маркетинга и рекламы ведет непосредственную работу с информацией о планах и объемах реализации продукции (услуг связи), анализу конкурентоспособности предоставляемых сервисов, и др., для осуществления своей деятельности. Данные информационные потоки относятся к

коммерческой тайне предприятия, и могут представлять потенциальный интерес для злоумышленников. Сам по себе отдел имеет связи с направлениями:

служба безопасности - разграничение доступа к конфиденциальной информации, направление отчетности о работе с защищенными информационными потоками по требованию;

Отдел бухгалтерского учета и аудита обрабатывает сведения о финансовой стороне деятельности предприятия, сведения о размере прибыли и себестоимости предоставленных услуг связи, и другие сведения экономического аспекта организации. Активное взаимодействие ведется со следующими структурными единицами:

отдел биллинговых систем - сбор информации об объемах предоставленных услуг, количестве введенных и выведенных из системы средств; учет количества и стоимости затраченных телекоммуникационных ресурсов по типам предоставляемых сервисов;

отдел кадров - получение информации о штате сотрудников организации, занимаемых должностях, рабочем времени, для проведения расчетов с персоналом за объем выполненной работы;

служба безопасности - предоставление данных о результатах проведенных аудитов средств и материально-технической базы организации;

административный отдел - получение указаний по координации действий с другими структурами оператора.

Таким образом, данные, передаваемые в некоторых информационных потоках этого отдела, также подпадают под категорию конфиденциальных.

Отдел кадров преимущественно обрабатывает персональные данные сотрудников организации, притом, по большей части, информация данного типа не выходит за пределы самого отдела. Исключением является отдел кадров, в который направляются сведения о персонале организации. С остальных позиций, подобно другим отделам организации, направлением установлены информационные связи со службой безопасности, куда по требованию передаются сведения о сотрудниках для проведения внешних и внутренних проверок актуальности поставленной информации; а также административным отделом, для получения указаний по взаимодействию совместно с другими структурными единицами предприятия.

Отдел мониторинга занимается сбором и обработкой исключительно статистической информации о предоставленных услугах, для предоставления остальным подразделениям по требованию. Данные носят информационный характер и в большинстве своем предназначены исключительно для использования внутри организации. Тем не менее, работа отдела не предполагает обработку конфиденциальной информации, таким образом исключая ее случайное или умышленное раскрытие.

Информационные связи с отделом безопасности и административным отделом сохраняются.

Тема 2. Средства защиты информации

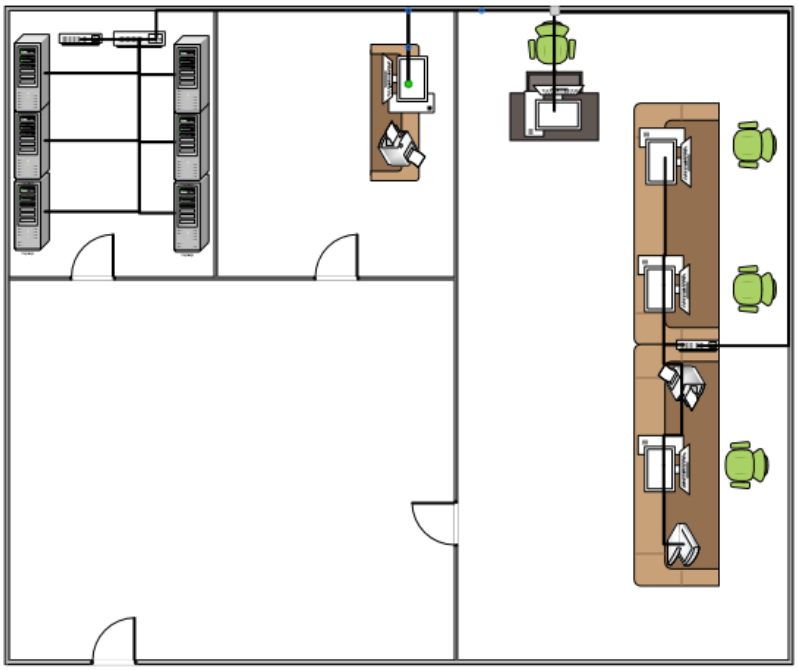


Рисунок 1 Общая схема сети на предприятии

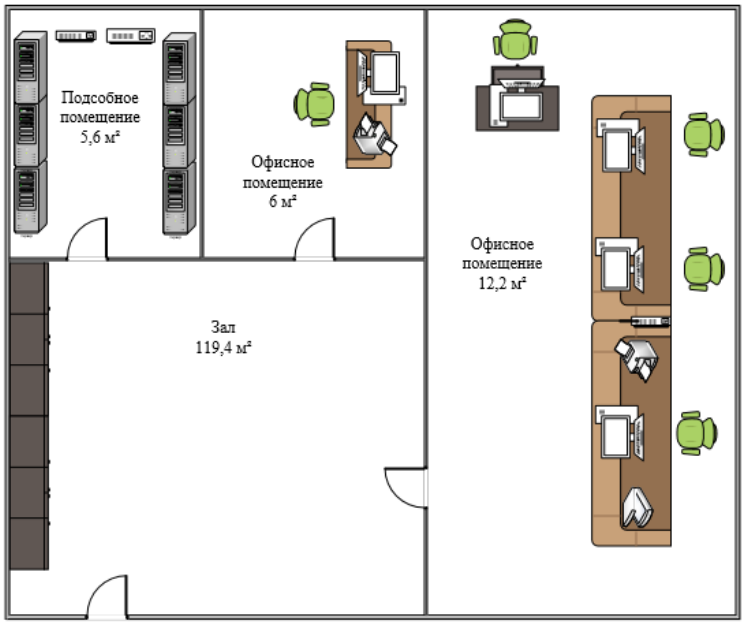


Рисунок 2 План помещения с размерами

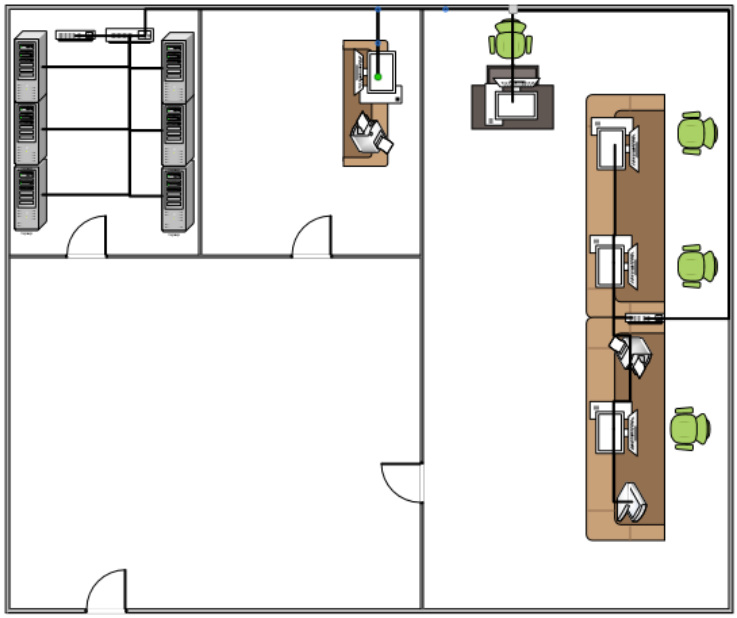


Рисунок 3 Схема прокладки сетевых трасс на предприятии

Спецификация и смета фрагмента сети ПАО "МегаФон Ритейл"					
№	Метериалы	Ед. изм.	Кол-во	Цена, руб	Стоимость, руб
1	L-UTP5E-10, Патч-корд UTP CAT5E 10m	Метр	5	410р	2050
2	Коммутатор D-Link Metro Ethernet DES-1210-10/ME/B1A Grey/Black	Единица	2	16943р	33886
3	Маршрутизатор Триколор TR-3G/4G-router-02 (046/91/00054231) 3G/4G	Единица	1	10977р	10 977
4	Лазерный принтер Xerox Phaser 3020BI	Еденица	2	13960р	27920
5	Сканер Canon Canoscan LIDE 400 Black	Еденица	1	16298р	16 298
6	Сервер LENOVO ST550 8SFF	Еденица	6	130208р	781248
	Итого, руб.:				872 379

Рисунок 4 Спецификация и схема фрагмента сети

В ходе прохождения (преддипломной) практики мною было выявлено, что в предприятие ПАО «МегаФон Ритейл» находится 1 локальная сеть и

имеются 5 рабочих станций, а также данное предприятие использует топологию сети «Звезда»

В ПАО «МегаФон Ритейл» находится 6 действующих серверов, а именно:

Рисунок 5 Сервер LENOVO ST550 8SF

Технические характеристики:

Процессор
1x Intel Xeon Gold 5115 Gold 5115 (10C Cache L3 13,75M Cache 2.40 GHz)

Оперативная память
16Гб 1x 16GB DDR4 1Rx4 PC4-2666V-R USED
(Поддержка до 768GB максимально, 12 DIMM ports)

RAID controller
Raid Lenovo 530-8i (2x Int. mSAS HD) 12Gbps PCI-E FH

Объем кэша контроллера, Мб
2000

Модуль удаленного управления
IMM2 Advanced

HDD
SSD 480GB Samsung PM893 SATA NEW (8 HDD 2.5")

Размеры (Ш x Г x В)
272 x 667 x 437

Форм-фактор
Tower

Вес
36

Блок питания
2x Lenovo 550W

Сетевая карта
Integrated Network Interface Lenovo Ethernet 2port 1Gb

Рельсы в стойку
нет

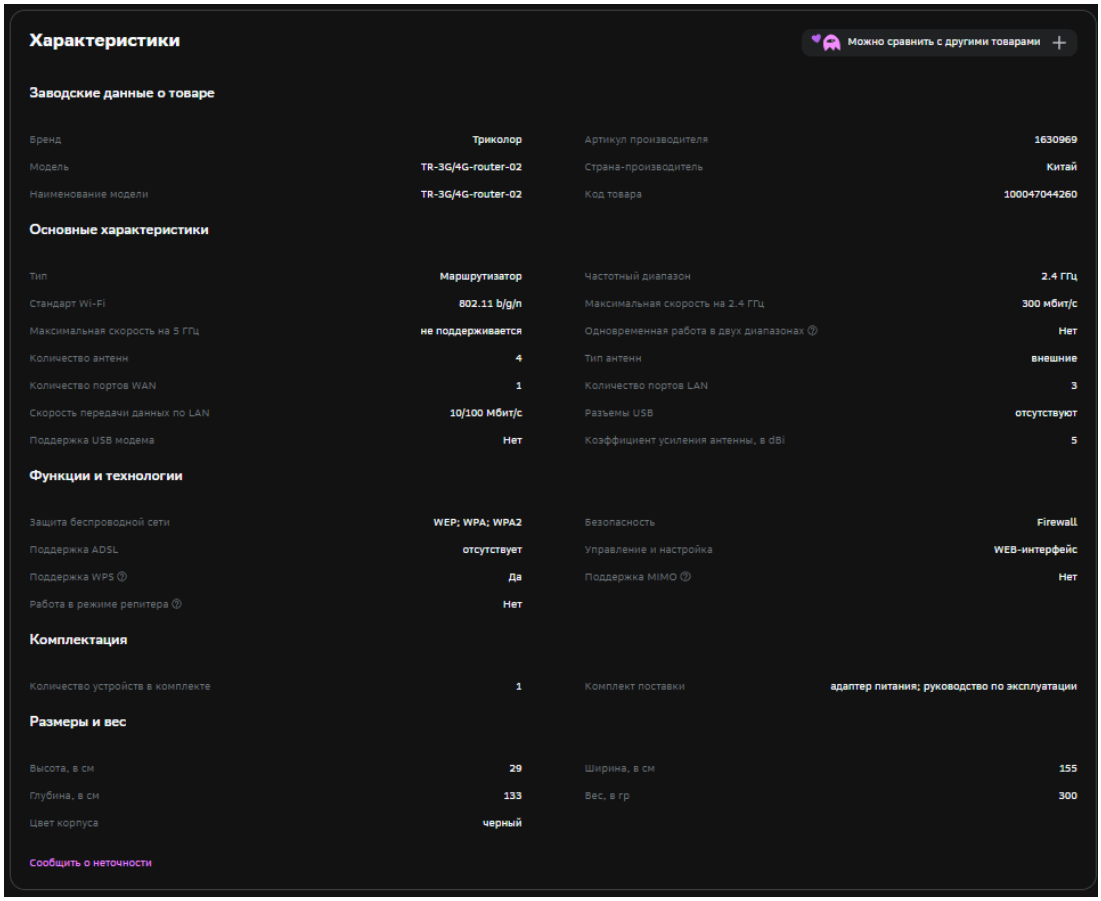
Рисунок 6 Технические характеристики сервера Сервер LENOVO ST550 8SFF

Тема 3. Аппаратное обеспечение компьютерной сети

Рисунок 7 Маршрутизатор Триколор TR-3G/4G-router-02 (046/91/00054231) 3G/4G

Данное устройство, принимает сетевой сигнал от провайдера и передает этот сигнал всем домашним устройствам. Грубо говоря, современный маршрутизатор получает интернет и «раздает» его подключенным девайсам.

Технические характеристики:



Характеристики

Можно сравнить с другими товарами

Заводские данные о товаре

Бренд	Триколор	Артикул производителя	1630969
Модель	TR-3G/4G-router-02	Страна-производитель	Китай
Наименование модели	TR-3G/4G-router-02	Код товара	100047044260

Основные характеристики

Тип	Маршрутизатор	Частотный диапазон	2.4 ГГц
Стандарт Wi-Fi	802.11 b/g/n	Максимальная скорость на 2.4 ГГц	300 мбит/с
Максимальная скорость на 5 ГГц	не поддерживается	Одновременная работа в двух диапазонах ⓘ	Нет
Количество антенн	4	Тип антенн	внешние
Количество портов WAN	1	Количество портов LAN	3
Скорость передачи данных по LAN	10/100 Мбит/с	Разъемы USB	отсутствуют
Поддержка USB модема	Нет	Коэффициент усиления антенны, в dBi	5

Функции и технологии

Защита беспроводной сети	WEP; WPA; WPA2	Безопасность	Firewall
Поддержка ADSL	отсутствует	Управление и настройка	WEB-интерфейс
Поддержка WPS ⓘ	Да	Поддержка MIMO ⓘ	Нет
Работа в режиме репитера ⓘ	Нет		

Комплектация

Количество устройств в комплекте	1	Комплект поставки	адаптер питания; руководство по эксплуатации

Размеры и вес

Высота, в см	29	Ширина, в см	155
Глубина, в см	133	Вес, в гр	300
Цвет корпуса	черный		

Сообщить о неточности

Рисунок 8 Тех. характеристики Маршрутизатора Триколор TR-3G/4G-router-02 (046/91/00054231) 3G/4G

Рисунок 9 Коммутатор D-Link Metro Ethernet DES-1210-10/ME/B1A Grey/Black

Данный прибор необходим для объединения несколько интеллектуальных устройств в локальную сеть для обмена данными. При получении информации на один из портов, передает ее далее на другой порт, на основании таблицы коммутации или таблицы MAC-адресов.

Технические характеристики:

Характеристики

Можно сравнить с другими товарами

Заводские данные о товаре

Артикул производителя	DES-1210-10/ME/B1A	Бренд	D-Link
Модель	DES-1210	Страна-производитель	китай
Наименование модели	dES-1210-10/ME/B1A	Код товара	100000576584

Основные характеристики

Тип	коммутатор	Вид	управляемый (layer 2)
Размещение	в стойку; настольное	Метод коммутации	store-and-forward
Тип разъемов	RJ-45; SFP	Количество LAN портов	8
Тип LAN портов	10/100 Base-TX	Количество Uplink портов	2
Тип Uplink портов	SFP	Внутренняя пропускная способность, в Гбит/с	5.6
Размер таблицы MAC адресов	8000	Максимальное количество VLANs	4000
Поддержка сетевых стандартов	IEEE 802.1d; IEEE 802.1p; IEEE 802.1q; IEEE 802.1s; IEEE 802.1v; IEEE 802.1w; IEEE 802.1x; IEEE 802.3ad; IEEE 802.3ah		

Функции и технологии

Поддержка PoE	отсутствует	Протоколы управления	IGMP; SNMP; Telnet; Web-интерфейс
Работа в стеке	Да	Другие поддерживаемые технологии	IPv6
Совместимость с операционными системами	Linux; MacOS; Windows 10; Windows 7; Windows Vista; Windows XP	Консольный порт	Да
Менеджмент порт	Нет		

Конструкция

Оперативная память, в МБ	128	Flash память, в Мб	16
Диапазон рабочих температур, в °C	0-50	Диапазон рабочей влажности, в %	10-90
Потребляемая мощность, в Вт	9.235	Размеры (ВхШхГ), в см	4,4x28x18
Цвет корпуса	серый; черный		

Рисунок 10 Тех. характеристики Коммутатора D-Link Metro Ethernet DES-1210-10/ME/B1A Grey/Black

Рисунок 11 Сканер Canon Canoscan LIDE 400 Black

Сканер — устройство, выполняющее считывание расположенного на плоском носителе (чаще всего бумаге) изображения для передачи информации на расстояние или для преобразования его в цифровой формат.

Технические характеристики:

Характеристики

Можно сравнить с другими товарами

Заводские данные о товаре

Модель	Canoscan LIDE 400	Бренд	Canon
Артикул производителя	2996C010	Страна-производитель	Китай
Наименование модели	LIDE400	Код товара	100023958569

Основные характеристики

Вид	планшетный сканер	Тип датчика	CIS
Разрешение сканирования, в DPI	4800x4800	Формат сканирования	A4
Максимальный размер сканирования, в мм	297x216	Скорость ч/б сканирования, в стр/мин	7.5
Скорость цветного сканирования, в стр/мин	7.5	Внутренняя глубина цвета, в битах	24
Внешняя глубина цвета, в битах	48	Количество оттенков серого	256
Устройство автоподачи	отсутствует	Двухстороннее сканирование	Нет
Источник света	светодиодная лампа	Подключение	проводное
Интерфейс подключения	USB		

Функции

Совместимость с операционными системами	Windows; Linux

Конструкция

Дисплей	Нет	Цвет корпуса	черный
Источник питания	usb		

Комплектация

Комплект поставки	USB-кабель; Диск с ПО

Размеры и вес

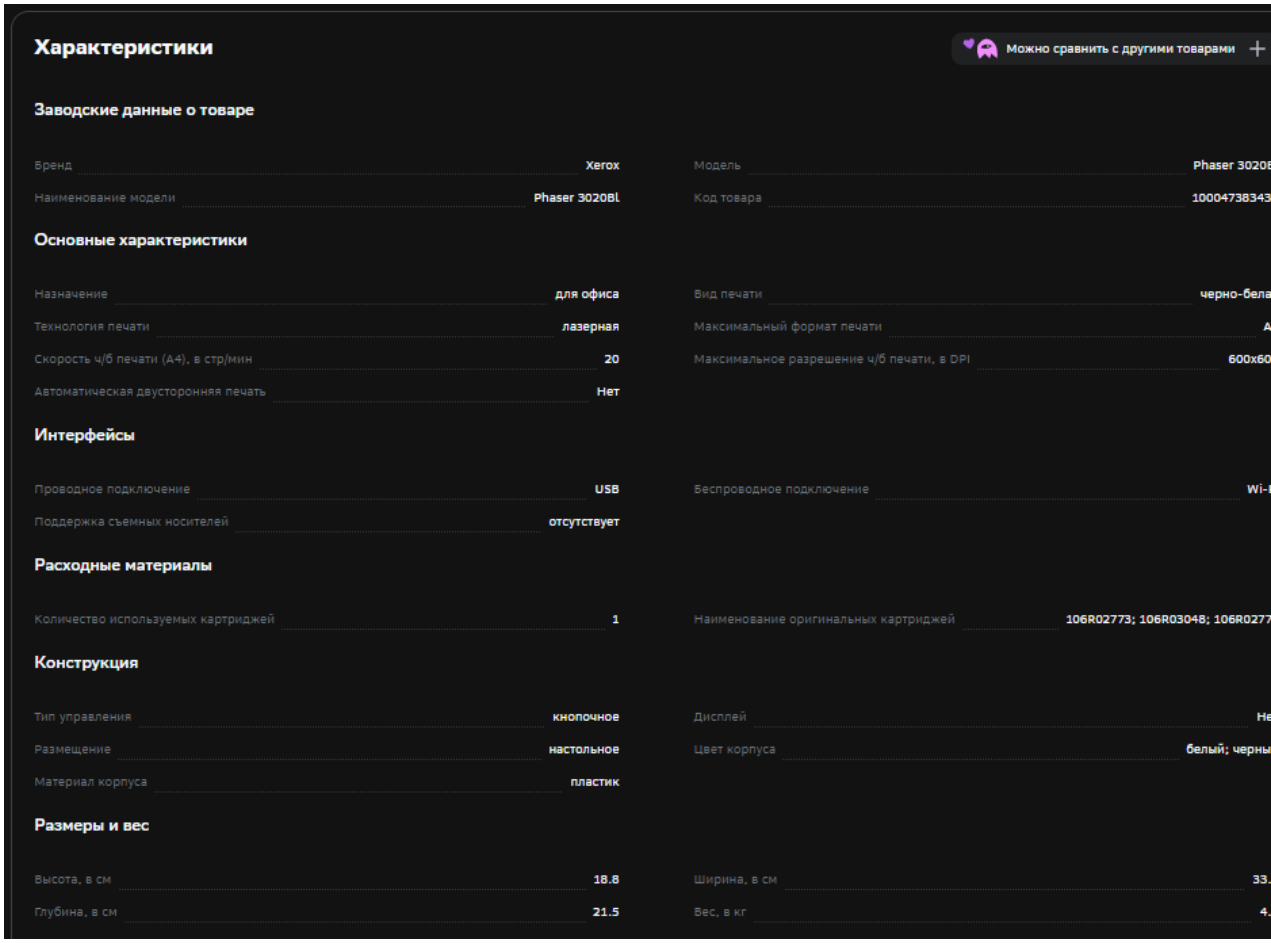
Высота, в см	3.9	Ширина, в см	25
Глубина, в см	36.5	Вес, в кг	1.7

Рисунок 12 Тех. характеристики Сканер Canon Canoscan LIDE 400 Black

Рисунок 13 Лазерный принтер Xerox Phaser 3020Bl

Один из видов принтеров, позволяющий быстро изготавливать высококачественные отпечатки текста и графики на обычной (офисной) бумаге.

Технические характеристики:



Характеристики

Можно сравнить с другими товарами

Заводские данные о товаре

Бренд	Xerox	Модель	Phaser 3020
Наименование модели	Phaser 3020Bl	Код товара	10004738343

Основные характеристики

Назначение	для офиса	Вид печати	черно-бела
Технология печати	лазерная	Максимальный формат печати	A
Скорость ч/б печати (A4), в стр/мин	20	Максимальное разрешение ч/б печати, в DPI	600x60
Автоматическая двусторонняя печать	Нет		

Интерфейсы

Проводное подключение	USB	Беспроводное подключение	Wi-
Поддержка съемных носителей	отсутствует		

Расходные материалы

Количество используемых картриджей	1	Наименование оригинальных картриджей	106R02773; 106R03048; 106R027

Конструкция

Тип управления	кнопочное	Дисплей	Не
Размещение	настольное	Цвет корпуса	белый; черны
Материал корпуса	пластик		

Размеры и вес

Высота, в см	18.8	Ширина, в см	33.
Глубина, в см	21.5	Вес, в кг	4.

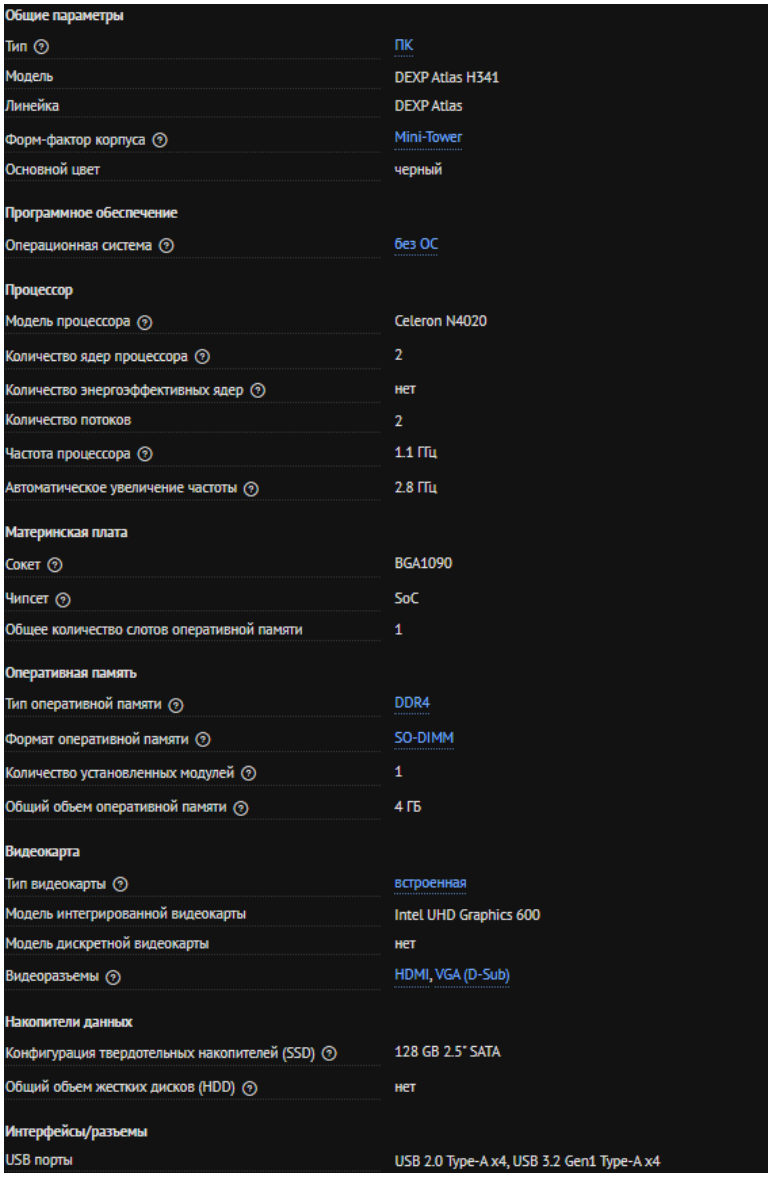
Рисунок 14 Тех. характеристики Лазерного принтера Xerox Phaser 3020Bl

Рабочая станция:

Рисунок 15 ПК DEXP Atlas H341

Устройство, предназначенное для автоматизации процессов обработки информации, в котором аппаратура работает под управлением определяющих её действия программ.

Технические характеристики:



Общие параметры	
Тип	ПК
Модель	DEXP Atlas H341
Линейка	DEXP Atlas
Форм-фактор корпуса	Mini-Tower
Основной цвет	черный
Программное обеспечение	
Операционная система	без ОС
Процессор	
Модель процессора	Celeron N4020
Количество ядер процессора	2
Количество энергоэффективных ядер	нет
Количество потоков	2
Частота процессора	1.1 ГГц
Автоматическое увеличение частоты	2.8 ГГц
Материнская плата	
Сокет	BGA1090
Чипсет	SoC
Общее количество слотов оперативной памяти	1
Оперативная память	
Тип оперативной памяти	DDR4
Формат оперативной памяти	SO-DIMM
Количество установленных модулей	1
Общий объем оперативной памяти	4 ГБ
Видеокарта	
Тип видеокарты	встроенная
Модель интегрированной видеокарты	Intel UHD Graphics 600
Модель дискретной видеокарты	нет
Видеоразъемы	HDMI, VGA (D-Sub)
Накопители данных	
Конфигурация твердотельных накопителей (SSD)	128 GB 2.5" SATA
Общий объем жестких дисков (HDD)	нет
Интерфейсы/разъемы	
USB порты	USB 2.0 Type-A x4, USB 3.2 Gen1 Type-A x4

Рисунок 16 Тех. характеристики ПК DEXP Atlas H341

Тема 4. Настройка и подключение рабочей станции к компьютерной сети предприятия

В процессе прохождения (преддипломной) практики мною было подключено и настроено 5 рабочих станций к одной локальной сети, пример таблица 1:

Таблица 1 Параметры задаваемые при настройке локальной сети

Наименование устройства	Задаваемые параметры при настройке локальной сети
Исходная машина	-
Роутер	192.168.1.1
Свитч	192.168.1.2
Рабочая станция №1	192.168.1.101
Рабочая станция №2	192.168.1.6
Рабочая станция №3	192.168.1.5
Рабочая станция №4	192.168.1.4
Рабочая станция №5	192.168.1.3

В ходе настройки локальной сети мною были выполнены следующие действия:

- Выбор подходящего сетевого компонента (свитч (switch), роутер (router)). В нашем случае присутствует и свитч и роутер
- Подключаем рабочие станции с помощью провода патч-корда
- Далее необходимо настроить обнаружения машин между собой
- Для этого проходим по пути: Панель управления — Система и безопасность — Система — Дополнительные параметры системы — Свойства системы. В открывшемся окошке надо указать, что компьютер является членом определенной рабочей группы и дать ей название. Это действие повторить на всех остальных ПК из сети.
- После этого настраиваем параметры общего доступа. Идем в «Центр управления сетями и общим доступом» и открываем «Изменить дополнительные параметры общего доступа». Там нужно включить сетевое обнаружение, а также доступ к файлам и принтерам.
- Теперь наступает важный этап работы: настроить сетевое обнаружение и общий доступ к файлам

- Важно убедиться, чтобы у всех компьютеров были правильные IP-адреса. Обычно система автоматически настраивает данный параметр, но если при работе LAN появятся сбои, то нужно будет указать адреса вручную. Проверить IP можно с помощью «настроек параметров адаптера». Заходим в «Центр управления сетями и общим доступом» и оттуда нажимаем «Изменение параметров адаптера».

- Нажимаем ПКМ по подключению и открываем свойства. Дальше открываем свойства IP версии 4 TCP / IPv4 (может иметь название «протокол Интернета версии 4»). IP-адрес — то, что нам нужно. Смотрим, чтобы у первого компьютера был адрес, отличный от второго. Например, для первого будет 192.168.0.100, 192.168.0.101 у второго, 192.168.0.102 у третьего и т.д. Для каждого последующего подключенного компьютера меняем последнюю цифру адреса. Стоит учесть, что у разных роутеров могут быть разные, отличные от указанных IP-адреса. На этом этапе локальная сеть уже готова и функционирует.

Тема 5. Организация доступа к ресурсам компьютерной сети.

Просмотр доступных ресурсов сети осуществляется в папке «Сетевое окружение». В окне этой папке можно увидеть общие ресурсы сети, к которой подключён компьютер. Для того, чтобы увидеть все компьютеры, подключенные к рабочей группе, выбираем в меню «Пуск» пункт «Сеть». Дважды щёлкнув мышью по любому из удалённых компьютеров в окне «Сетевое окружение», можно узнать какие ресурсы сети доступны для работы. Для того, чтобы другие пользователи сети могли обращаться к вашему компьютеру необходимо открыть им сетевой доступ для работы с вашими ресурсами.

Можно открыть доступ пользователям к дискам вашего компьютера. Это даст им возможность редактировать и сохранять файлы, размещённые на этих дисках. Чтобы это сделать, необходимо выполнить следующие действия:

Открыть системную папку компьютера и выбрать из контекстного меню пункт «Свойства». В открывшемся окне выбрать вкладку «Доступ» и в ней нажать на кнопку «Расширенная настройка»

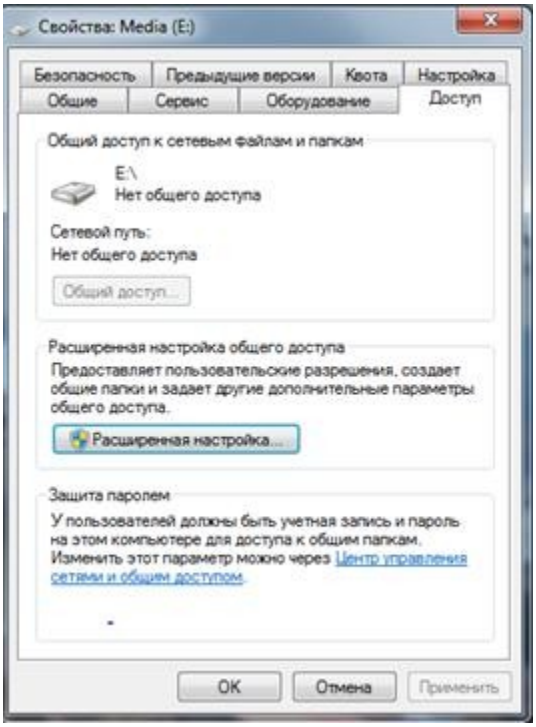


Рисунок 1 - Открытие общего доступа к папке в локальной сети

В открывшемся окне поставить галочку напротив «Открыть общий доступ к этой папке». Также ниже можно задать количество одновременных пользователей, которые могут получить доступ к этой папке. После этого нажать на кнопку ОК

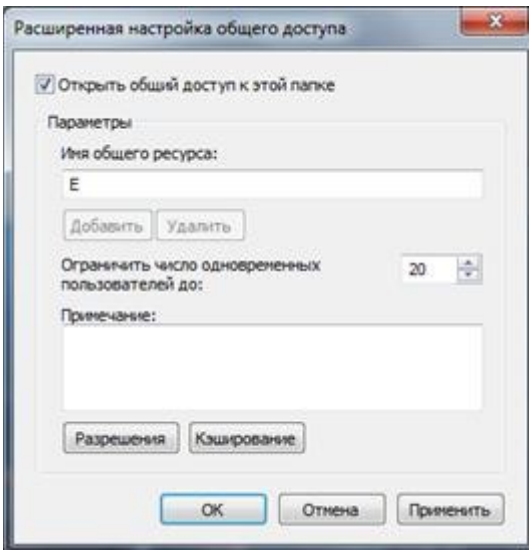


Рисунок 2 - Открытие общего доступа к папке в локальной сети

Для выбора прав доступа к общему диску необходимо в окне «Свойства» выбрать вкладку «Безопасность». В открывшемся окне нажать на кнопку «Изменить»

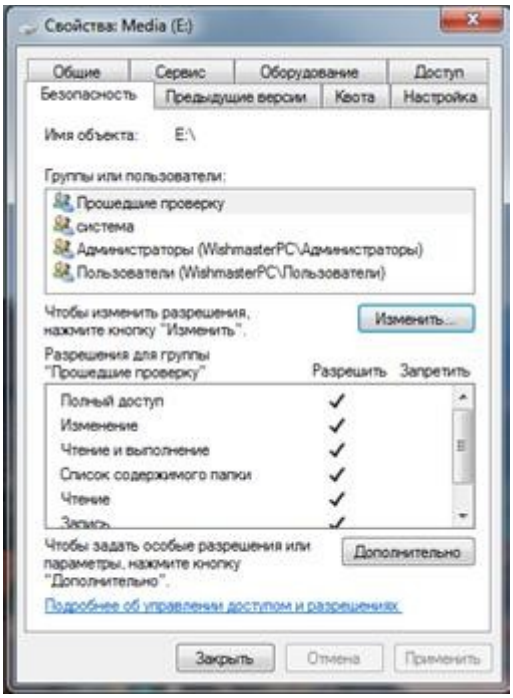


Рисунок 2 - Открытие общего доступа к папке в локальной сети

В открывшемся окне диалога можно установить пользователей и их права.

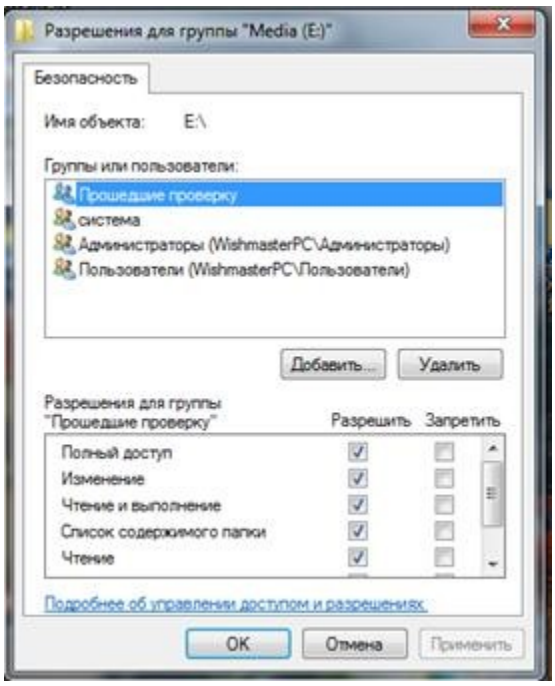


Рисунок 3 - Открытие общего доступа к папке в локальной сети

Чтобы открыть какую-либо папку для общего доступа в сети, необходимо нажать правой кнопкой мыши на этой папке и выбрать из меню «Свойства» команду «Общий доступ». Далее выполняются все действия, аналогичные действиям с назначением общего доступа к диску.

Для открытия пользователям локальной сети доступа к сетевому принтеру, который подключен к вашему компьютеру, выполните следующую последовательность действий:

Запустите меню «Пуск» – Панель управления – Принтеры и факсы.

Правой кнопкой мыши нажмите на значке принтера, подключенного к вашему компьютеру, зайти в меню «Свойства принтера» и выбрать там пункт «Общий доступ». На вкладке «Доступ» выбрать галочку «Общий доступ к данному принтеру», и нажать клавишу ОК

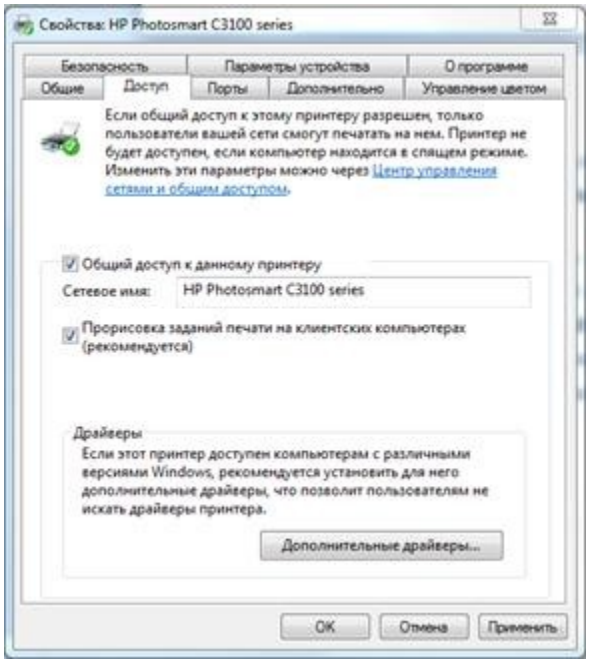


Рисунок 4 - Открытие общего доступа к сетевому принтеру

Теперь этот принтер можно использовать для распечатки документа с любого компьютера сети.

Очень часто возникает потребность получить определённый файл в сети, даже если компьютер, на котором лежит этот файл, выключен или недоступен. В таком случае можно использовать так называемую функцию автономных файлов и папок. Такие папки сохранятся на локальный диск и являются доступными в сети в любой момент времени. Чтобы воспользоваться этой функцией, необходимо в процессе работы сети выбрать необходимую для автономного доступа папку, нажать на ней правой кнопкой мыши и из раскрывшегося меню выбрать опцию «Всегда доступны в автономном режиме».

Наличие локальной сети в компьютерном классе открывает множество новых возможностей, таких, как:

- Пересылать файлы с одного компьютера на другой
- Запускать на компьютере папки, файлы и даже операционные системы удалённо.
- Использовать принтеры таким образом, как будто они подключены к вашему компьютеру.
- Осуществлять выход в интернет для компьютеров всего класса.

Программа MERITS. Эта программа является разработкой сингапурских программистов для управления компьютерным классом. Поддерживает большое количество возможностей, такие, например, как включение компьютера учителя удаленно.

Тема 6. Разработка и утверждение плана технического задания на создание или модификацию ИС в защищенном исполнении.

Защищенная информационная система (ЗИС) – это информационная система, обеспечивающая защиту от несанкционированного доступа, копирования, изменения и уничтожения информации, хранящейся в системе. Создание или модификация ЗИС требует разработки и утверждения плана технического задания, который определяет требования и условия на создание или модификацию системы.

Основные этапы разработки и утверждения плана технического задания на создание или модификацию ЗИС:

- Определение требований к системе: определение целей и задач, которые должна решать система, а также требований к безопасности и конфиденциальности информации.
- Анализ существующих решений: изучение доступных на рынке решений, определение их преимуществ и недостатков, выбор наиболее подходящего решения.
- Разработка технического задания: составление документа, в котором описываются требования к системе, ее функциональные возможности, а также требования к безопасности и конфиденциальности информации.
- Утверждение технического задания: согласование документа с заинтересованными сторонами, а также получение разрешений и лицензий на создание или модификацию системы.
- Разработка и внедрение системы: создание и настройка системы на основе технического задания, тестирование, обучение пользователей и запуск системы в эксплуатацию.

Базовые требования к ЗИС:

- Классификация информации: определение уровня конфиденциальности информации и ее классификация согласно установленным правилам.
- Контроль доступа: обеспечение контроля доступа к информации, ограничение прав доступа к данным, аутентификация пользователей, защита от несанкционированного доступа.
- Шифрование данных: использование средств шифрования для защиты информации при ее передаче или хранении.
- Мониторинг: обнаружение и предотвращение несанкционированного доступа, мониторинг событий в системе и реакция на инциденты безопасности.

- Резервное копирование: создание резервных копий данных и системы, чтобы обеспечить возможность восстановления информации в случае ее потери или повреждения.
- Физическая защита: обеспечение физической защиты серверов и сетевого оборудования, а также ограничение доступа к помещениям, где хранится оборудование.
- Обучение и аудит: обучение пользователей правилам безопасности и проведение аудита системы с целью выявления уязвимостей и недостатков.

Способ проведения аудита зависит от задач и уровня угрозы. Чем меньше компания и ниже продвинутость используемых технологий, тем меньше интерес злоумышленников и проще оценка. Важное условие перед началом аудита — составление технического задания на работающую систему информационной безопасности: и руководство компании и аудитор должны представлять, как будет работать идеальная в их понимании служба.

Любой аудит состоит из обязательных этапов. Определение границ и глубины оценки — на этом этапе руководство компании решает, в каких областях из перечисленных выше проводить обследование. Оптимальный вариант — сделать оценку по всем направлениям и максимально глубоко, но всегда встает вопрос соответствия затрат и экономической эффективности применения полученных данных.

Один из способов сокращения разного вида затрат — сужение зоны оценки до типовых блоков.

Например, если в разных подразделениях схожие информационные системы, высока вероятность, что в них присутствуют одинаковые уязвимости.

Проверив полностью один филиал компании, остальные можно обследовать уже только на ошибки, обнаруженные в первом.

Второй этап — сбор и систематизация данных о видах информации, которая возникает, хранится и передается внутри компании, и которой обмениваются с внешними контрагентами. На этом же этапе проводят инвентаризацию всех технических и программных средств, используемых для генерации, хранения и передачи данных. Далее следует этап обследования информационных процессов. Здесь очень много подпунктов и желательно не упустить ни один из них. Лучше всего, если человек, проводящий аудит, будет обследовать прохождение процессов прямо на рабочих местах, а не со слов исполнителей.

В ходе этапа определяют участников информационных процессов, как они проходят, какие ресурсы используют, требуемые согласования. По сути,

процедура ничем не отличается от описания других бизнес-процессов в компании.

Далее основные пункты этого этапа, которые нужно проанализировать:

- как с информацией работает персонал;
- как происходит обучение сотрудников по обеспечению безопасности;
- кто и как управляет доступом к информации;
- понятие и документальное оформление тайны и конфиденциальной информации на предприятии;
- как обеспечивается защита от вредоносных программ;
- кто и как отслеживает события в сфере безопасности, как на них реагируют;
- алгоритмы шифрования данных, генерация, хранение и ликвидация паролей как происходит архивация, восстановление, дублирование данных;
- как используют мобильные, переносные, съемные устройства хранения данных;
- организация доступа в интернет и использования электронной почты в компании;
- как происходит доступ к информации для лиц, не являющихся сотрудниками;
- как контролируется доступ к сети внутри организации и извне.

Следующим шагом оценивают техническое и программное обеспечение: сетевое оборудование и компьютеры, базы данных, антивирусы и сетевые экраны, операционные системы на сервере и локальных машинах, средства интернет-коммуникации и другие пользовательские программы и приложения.

Важно исследовать состояние не только виртуальных хранилищ, но и физических — архивные комнаты, сейфовое оборудование, в том числе, охранные и противопожарные сигнализации и средства. На пятом этапе, когда создана целостная картина «как есть», ее сравнивают с тем, как надо, то есть с техническим заданием на структуру и функции безопасной информационной системы. В ходе этапа выявляют слабые места, ищут уязвимости и определяют риски.

Последний этап аудита — отчет для руководства (заказчика) с указанием недостатков и степени их опасности. Возможно составление плана первоочередных мероприятий по борьбе с высокорисковыми угрозами.

Для небольших предприятий наибольшую опасность с точки зрения информационных уязвимостей представляют сотрудники и банальная халатность в отношении простых правил. Например, часто предприниматели опасаются передавать ведение собственной бухгалтерии на аутсорс, полагая,

что бухгалтер в штате надежнее и безопаснее. Это серьезное заблуждение — узнайте, как бухгалтеры разоряют компании и что делать, чтобы обезопасить себя.

Этапы проведения аудита

Проведение аудита информационной безопасности включает в себя несколько этапов:

- Подготовительный этап. На этом этапе определяются цели и задачи аудита, а также формируется команда, которая будет проводить аудит.
- Сбор информации. На этом этапе аудиторы собирают информацию о системе защиты информации, изучают документацию, протоколы и журналы системы, а также проводят интервью с сотрудниками, ответственными за информационную безопасность.
- Анализ собранной информации. На этом этапе аудиторы анализируют собранную информацию и оценивают эффективность системы защиты информации.
- Проверка соответствия законодательству и стандартам. На этом этапе проводится проверка соответствия системы защиты информации законодательству и стандартам безопасности.
- Выявление уязвимостей и возможных угроз безопасности. На этом этапе аудиторы выявляют уязвимости и возможные угрозы безопасности системы защиты информации.
- Подготовка отчета. По результатам аудита составляется отчет, в котором указываются выявленные уязвимости и возможные угрозы безопасности, а также рекомендации по усовершенствованию системы защиты информации.
- Дополнительные рекомендации:
- Важно выбрать правильных аудиторов, которые обладают опытом и знаниями в области информационной безопасности.
- Проведение аудита должно быть регулярным процессом, который позволяет поддерживать систему защиты информации в актуальном состоянии.
- Отчет по результатам аудита должен быть доступен только ответственным лицам, чтобы предотвратить утечку информации.
- После проведения аудита следует принять меры для устранения выявленных уязвимостей и угроз безопасности.
- В итоге, проведение аудита информационной безопасности является необходимым процессом для обеспечения безопасности информационных систем и защиты конфиденциальной информации.

Тема 7. Обоснование предварительных проектных решений по ИС.

Информационное обеспечение (ИО) включает в себя:

систему классификации и кодирования;

систему унифицированной документации, используемой в ИО;

информационную базу.

Классификатор - это систематизированных свод наименований группировок объектов, признаков и их кодовых обозначений. Классификаторы служат средством описания данных, обуславливают единство классификации и кодирования информации и предназначены для обеспечения машинной обработки и выдачи данных в удобной форме потребителям при решении различных задач. В зависимости от применения они делятся на три группы:

- общегосударственные классификаторы,
- отраслевые (ведомственные) классификаторы, используемые в пределах определенной отрасли (ведомства);
- локальные классификаторы, используемые в пределах организации или группы организации.

Значительную долю вне машинного ИО составляет документация. В условиях автоматизации важное значение придается унификации документации, устанавливающей единые требования к содержанию и построению документов. Унифицированные формы документов вырабатываются как для всех предприятий РФ (например, формы бухгалтерской отчетности), так и для отдельных предприятий (например, формы управленческой отчетности). Унификация заключается в тщательном отборе и четком определении необходимой номенклатуры документов. При этом определяются сферы назначения и использования документов и выявляются специфические особенности, характерные для соответствующих видов документов. Документы могут быть унифицированными и локальными.

В данном дипломном проекте использованы локальные документы: «Заявка на закупку материальных ценностей», «Заявка на регистрацию пользователя и доступ к программным ресурсам», «Заявка на устранение неполадок», «Заявка на доступ к сетевым ресурсам». Информационные файлы формируются на основе исходной информации, содержащейся в вышеуказанных первичных документах - основных носителях первичной экономической информации в системах машинной обработки данных. К ним предъявляется ряд требований:

- достаточная полнота информации для решения задачи;
- исключение избыточности информации;
- достоверность и своевременность информации;

- согласованность форм первичных документов с макетами размещения информации на машинном носителе;
- логичность построения документа;

Под файловой организацией ИБ понимается локальное размещение базы на компьютере, доступ к которому других пользователей осуществляется стандартными методами ОС для обмена данными по сети, например в MS Windows это Sharing и Security, что уменьшает скорость обработки данных в локальной базе. Под смешанной организацией ИБ подразумевается распределённая база данных, хранящаяся на нескольких серверах и реплицирующая изменения в каждой из них по расписанию, данная структура ИБ используется в системах класса ERP для работы в одной ИБ территориально удалённым офисам одновременно.

Интегрированный способ организации ИБ представляет собой совокупность взаимосвязанных и хранящихся вместе данных при такой минимальной избыточности, которая допускает их использование оптимальным образом для любых приложений и при этом обеспечивается независимость данных от программы, а для актуализации данных используется общий способ управления

В данном дипломном проекте наиболее целесообразной организацией ИБ считаю интегрированную организацию ИБ, так как размер базы будет увеличиваться каждый день на 700-800 записей. И оптимальным выбором будет использование СУБД вместо файлового хранения базы данных

Существует три модели логической структуры базы данных (по способу установления связей между данными): иерархическая, сетевая и реляционная.

В иерархической модели каждой информационной единице (сегменту), кроме корневого, соответствует один исходный сегмент и между исходным и порожденным сегментом устанавливается только одна связь. В иерархических моделях экземпляру исходного сегмента соответствует в общем случае какое-то число экземпляров порожденного сегмента. Такие структуры удобны для отображения отношений типа «один ко многим» в предметной области. Просмотр иерархической структуры возможен только с корневой вершины. Пропуск сегмента в иерархическом пути при доступе к заданному сегменту не допускается. Основные недостатки иерархической структуры: трудность (неэффективность) отображения отношений типа «многие ко многим»; длительность доступа к сегментам, находящимся на нижних уровнях иерархии; ориентированность на определенный тип (разрез) запроса.[19]

Сетевые модели графически отображаются в виде графа. Вершинам графа соответствуют составные единицы информации (записи). Экземпляры записей образуют файлы. Структура записи может быть иерархической или линейной в зависимости от системы. Между парой типов записей может быть объявлено несколько связей, имена и направления связей должны быть четко обозначены.

Недостатками являются: сложность (очень большое число параметров описания данных и операторов), а также неудобство навигационного доступа.[19]

Реляционная база данных - это множество отношений. Реляционная модель основана на математической логике и является простейшей и наиболее привычной формой представления данных в виде таблицы. Строка таблицы эквивалентна записи файла базы данных, а колонка - полю записи. Доступ к элементу данных осуществляется посредством связи требуемой строки (записи) с требуемой колонкой (полем). Достоинством реляционной модели является сравнительная простота инструментальных средств ее поддержки, недостатком - жесткость структуры данных (например, невозможность задания строк таблицы произвольной длины) и зависимость скорости ее работы от размера базы данных.

Преимущества использования реляционных базы данных состоит в следующем:

Простота - в реляционной модели данных существует всего одна информационная конструкция, которая формализует табличное представление данных, привычное для пользователей;

Теоретическое обоснование - наличие теоретически обоснованных методов нормализации отношений позволяет получать базы данных с заранее заданными свойствами (в основном, с гарантией минимальной избыточности представления данных);

Независимость данных - когда необходимо изменить структуру реляционной базы данных, то это приводит к минимальным изменениям в программном продукте.

Моделью логической структуры базы данных была выбрана именно реляционная , так как она позволяет довольно быстро сформировать связи между таблицами для правильного построения запросов к базе данных и также легко разорвать эти связи и создать новые для построения другого запроса. Кроме того архитектура построения связи более проста и время выполнения запроса в реляционной модели выше чем при использовании сетевой или иерархической структуры.

Исходные сведения для решения обозначенной задачи получают из таких документов, как:

- электронное письмо от сотрудника компании \c описанием неисправности на неформальном языки в сфере ИТ
- регламент работы службы горячей линии
- ежедневное письмо о присутствии Сотрудников IT по всем направлениям.

- письма, регламентирующие изменения ответственных по классифицированным направлениям инцидентам и новым направлениям

Результаты решения задачи отображаются в таких отчетах и документах, как:

- Отчет по согласованным заявках
- Отчет заявок по местоположению заявителя
- Отчет о логике назначения заявителя.

Для решения поставленной задачи задействованы такие классификаторы объектов, как: города, регионы, улица, код описания неисправности

В таблице 6 представлено описание используемых классификаторов.

Описание используемых классификаторов.				
Наименование кодируемого множества объектов	Значимость кода	Система кодирования	Система классификации	Вид классификатора
Регион	4	Порядковая	Отсутствует	Локальный
Город	4	Порядковая	Отсутствует	Локальный
Улица	4	Порядковая	Отсутствует	Локальный
Код описания неисправности	4	Порядковая	Отсутствует	Локальный

Тема 8. Разработка предварительных проектных решений по ИС в защищенном исполнении.

В России существует огромное количество видов (категорий) информации, подлежащей защите (по некоторым оценкам до 30), и к каждому из них предъявляются свои требования по обеспечению безопасности, кроме того в связи с развитием информационных технологий постоянно растет сложность систем обработки данных.

В результате специалисты в области информационной безопасности сталкиваются с необходимостью защищать все более сложные системы в соответствии с разными, порой противоречивыми требованиями, и при этом сроки разработки СЗИ крайне ограничены.

В связи со всем вышесказанным особую актуальность приобретает создание средств поддержки разработки защищенных систем.

Разработка информационных систем в защищенном исполнении осуществляется следующим образом:

- формирование требований к информационной системе, в том числе обследование объекта защиты, определение факторов влияющих на информацию, разработка предварительных требований по защите информации;
- разработка концепции АС, в том числе формирование модели угроз информационной системы, определение принципов построения системы защиты;
- разработка технического задания на создание информационной системы в защищенном исполнении;
- разработка проектных решений (данная стадия может подразделяться на эскизное и техническое проектирование, разработку рабочей документации).

Далее следуют этапы по созданию и вводу в действие информационной системы в защищенном исполнении.

Проектирование информационных систем в защищенном исполнении осуществляется в несколько этапов:

- анализ информационной системы (определение актуальных угроз безопасности информационной системы и формирование требований к системе защиты информации);
- определение технического решения по защите информации (формирование модели защиты, определение состава применяемых средств и методов защиты);
- проверка решения на соответствие требованиям.

В процессе разработки информационной системы в защищенном исполнении формируется ряд прикладных моделей, характеризующих особенности конкретного объекта защиты (информационной системы). При формировании прикладных моделей:

- используются базовые модели, содержащие структурированную
- информацию, в том числе описания угроз безопасности, возможностей нарушителя, средств защиты.
- Рассматриваемая методика подразумевает автоматизированную разработку, т. е. формирование прикладных моделей средствами автоматизации на основании введенных данных. Вместе с тем

Рассмотрим процесс проектирования информационных систем в защищенном исполнении более детально.

Для определения необходимых и достаточных мер защиты информационных систем формируется модель угроз безопасности информационной системы. В ходе формирования модели угроз

Выявляется перечень угроз, актуальных для конкретной информационной системы. Модель угроз безопасности формируется на основе анализа объекта защиты – информационной системы.

При этом для определения перечня актуальных для конкретной информационной системы угроз безопасности необходимо провести анализ уязвимостей системы и возможностей нарушителя, т. е. сформировать прикладную модель нарушителя. При определении возможных атак необходимо учитывать, что атака, реализующая ту или иную угрозу, может происходить в несколько этапов, т. е. помимо защищаемых ресурсов должны быть определены

Потенциальные точки воздействия – элементы объекта защиты, посредством которых может быть проведена атака на защищаемую информацию.

Прикладная модель нарушителя в сочетании с прикладной моделью объекта определяет перечень возможных угроз безопасности информации; данный перечень может быть скорректирован экспертом в части уточнения потенциального ущерба и вероятности реализации угроз, после чего формируется перечень актуальных угроз безопасности – прикладная модель угроз.

Таким образом, в ходе анализа информационной системы должны быть сформированы следующие прикладные модели:

- Модель объекта защиты;
- Модель нарушителя;

- Модель угроз.

На основе прикладной модели угроз формируются требования к защите рассматриваемой информационной системы. При формировании перечня требований к системе защиты используется следующее правило: «Каждой актуальной угрозе безопасности должно соответствовать как минимум одно требование к методу (средству) противодействия». \

Требования к системе защиты информации в свою очередь определяют состав применяемых средств и мер защиты, которые описываются прикладной моделью защиты. Модель защиты должна предлагать способ нейтрализации для всех актуальных способов доступа.

Тема 9. Разработка рабочей документации на внедрение ИС

Разработка информационной системы (ИС) является достаточно сложным и долгим процессом, в ходе и результате которого появляется большое количество технической документации, содержащей описание создаваемого продукта с различных точек зрения. Техническая документация может включать в себя не только основание для разработки и руководства по эксплуатации готового программного продукта, но и другие артефакты, создаваемые на разных этапах разработки.

В нашем случае при работе с нашим предприятием необходимо сдать определенный пакет документов – руководств, инструкций, проектных решений, оформленных по требованиям нормативных документов.

Техническая документация является составляющей проекта по созданию, внедрению, сопровождению, модернизации и ликвидации информационной системы на всем протяжении жизненного цикла. Комплекс технических документов, который регламентирует деятельность разработчиков, называется нормативно-методическим обеспечением (НМО). В данный комплекс входят:

- стандарты;
- руководящие документы;
- методики и положения;
- инструкции и т. д.

НМО регламентирует порядок разработки, общие требования к составу и качеству программного обеспечения (ПО), связям между компонентами, определяет содержание проектной и программной документации.

Основным назначением технической документации является обеспечение эффективных процедур разработки и использования информационной системы как программного продукта, а также организация обмена между разработчиками и пользователями ИС.

Таким образом, можно выделить следующие функции технической документации:

- дает описание возможностей системы;
- обеспечивает фиксацию принятых и реализованных
- проектных решений;
- определяет условия функционирования ИС;
- предоставляет информацию об эксплуатации и обслуживании ИС;
- регламентирует процедуру защиты информации, регулирует права различных групп пользователей;
- определяет возможности модернизации системы.

Перед составлением технической документации необходимо иметь ответы на следующие вопросы:

- что и зачем должно быть документировано?
- для кого предназначен тот или иной документ?
- какие ошибки может допустить пользователь и что нужно сделать для их устранения?
- как и в каких условиях будет использоваться документ?
- каковы сроки разработки документа?
- как будет обновляться и поддерживаться документация, каковы механизмы и сроки внесения изменений и пересмотра документов, и кто ответственен за реализацию этих действий, а также за хранение, неизменность и контроль за исполнением?
- кто будет оценивать документ и как он соотносится с отраслевыми или ведомственными требованиями на сертификацию разработки?

Как правило, к технической документации предъявляются следующие основные требования:

- документы должны быть точными, полными и, по возможности, краткими, иметь четкое и однозначное толкование;
- документация должна создаваться параллельно с разработкой самой информационной системы;
- обязанности по документированию системы лежат на ее разработчике;
- для повышения эффективности работы с документами должны использоваться стандарты, регламентирующие форму и содержание документов.

Исходя из последнего требования к документации, необходимо рассмотреть основные стандарты, которые используются в области информационных систем на территории Российской Федерации.

В настоящее время существует несколько классификаций стандартов на проектирование и разработку информационных (автоматизированных) систем.

Классический способ классификации группирует стандарты по двум признакам:

По объекту стандартизации:

- стандарты на продукты и услуги;
- стандарты на процессы и технологии.

По предмету стандартизации:

- функциональные стандарты (стандарты на языки программирования, протоколы, интерфейсы);
- стандарты на организацию жизненного цикла (ЖЦ) автоматизированных систем и программного обеспечения.

В свою очередь официальные стандарты подразделяются на:

- международные стандарты (ISO, ANSI, IDEF0/1);
- стандарты Российской Федерации (ГОСТ);
- отраслевые стандарты;
- ведомственные стандарты.

Тема 8. Разработка внутренних нормативных документов по введению средств защиты информации в эксплуатацию.

Заключение

В ходе прохождения производственной практики мною были изучены информационные системы, меры и средства для их защиты, официальные документы предприятия, нормативная и методическая документация, которые позволили решить многие поставленные задачи.

В процессе прохождения производственной практики я ознакомился с организационной структурой, рассмотрел информационную систему обработки персональных данных, построил для неё модель угроз и модель нарушителя, и рассчитал актуальные угрозы информационной системы персональных данных. 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.

Список литературы

Основные источники:

1. Информационные технологии обеспечения конфиденциальности и сохранности данных: учеб. пособие/ Н.В. Титовская, С.Н. Титовский; Краснояр. гос. аграр. ун-т. – Красноярск, 2018. – 188 с.

2. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

3. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

4. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации. - М.: МО РФ, 1998. - 224 с.

5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: И НФ РА-М, 2011. — 416 с.: ил. — (Профессиональное образование).

Периодические издания:

1. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

3. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

4. Журналы Защита информации. Инсайд: Информационно-методический журнал

5. Информационная безопасность регионов: Научно-практический журнал

Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

2. Информационный портал по безопасности www.SecurityLab.ru.

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Российский биометрический портал www.biometrics.ru

5. Сайт журнала Информационная безопасность http://www.itsec.ru –