И.о. зам. директора по УиНМР
Н.В. Слюдовой
преподавателя Ванюшиной
Ольги Владимировны

ЗАЯВКА

Прошу направить меня на стажерскую практику по индивидуальной программе в ПАО «Арзамасский машиностроительный завод»

Период стажёрской практики с 24.02.2022 г. по 25.03.2022г.

Паспорт программы стажировки прилагается.

_____ _____
(подпись) *(расшифровка подписи)*
«_____»_____20____ г.

СОГЛАСОВАНО
Руководитель структурного
подразделения _____ _____
(подпись) *(расшифровка подписи)*

Министерство образования, науки и молодежной политики Нижегородской области
Государственное бюджетное профессиональное образовательное учреждение
«Арзамасский коммерческо-технический техникум»

СОГЛАСОВАНО
Руководитель предприятия
(организации)
_____
«__»_____20___ г.
М.П.

УТВЕРЖДАЮ
И.о. зам. директора по УиНМР
_____Н.В Слюдова
«___»_____20___ г.

ПРОГРАММА СТАЖИРОВКИ
преподавателя

УД ЕН.03 Информационные технологии в профессиональной деятельности

специальности 13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)

Ванюшиной Ольги Владимировны

Арзамас
2022г.

I. ПАСПОРТ ПРОГРАММЫ

1. Наименование УД, МДК (ПМ), в рамках которого предусмотрено прохождение стажировки	ЕН.03 Информационные технологии в профессиональной деятельности Специальность 13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)
2. Наименование программы стажировки	Развитие и совершенствование профессиональных компетенций по информационным технологиям специальности 13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)
3. Место прохождения стажировки	Нижегородская область, г. Арзамас, ул. 9 МАЯ, д. 2 ПАО «Арзамасский машиностроительный завод», отдел ИТ
4. Форма стажировки	без отрыва от основной работы
5. Срок стажировки	дата начала стажировки 24.02.2022 г. дата окончания стажировки 25.03.2022 г. приказ по стажировке: №6-лс/к от 24.02.2022
6. Количество часов	72 ч.
7. Цель стажировки	развитие и совершенствование профессиональных компетенций, изучение передового опыта
8. Задачи стажировки	С целью овладения профессиональными компетенциями *необходимо научиться:* - изучить основные направления деятельности отдела информационных технологий ПАО «Арзамасский машиностроительный завод»; - изучить конфигурацию и виды аппаратного и программного обеспечения отдела ИТ ПАО «АМЗ»; - усовершенствовать знания о функционировании компьютерной сети и сетевого оборудования; - изучить виды сетевых программных средств и способы сетевого администрирования отдела ИТ; - изучить сетевое взаимодействие между компьютерами локальной сети;

	- изучить основные виды сетевой информационной безопасности
9. Руководитель (консультант стажировки)	Васильев А.Б., начальник отдела информационных технологий ПАО «Арзамасский машиностроительный завод»
10. Контроль прохождения стажировки	Н.В. Слюдова, и.о. заместителя директора по УиНМР
11. Защита итогов стажировки	На заседании методического объединения

II. СОДЕРЖАНИЕ СТАЖИРОВКИ

№ п\п	Перечень основных вопросов, подлежащих изучению	Виды деятельности	Количество часов	Планируемые результаты
1.	Изучение характеристики предприятия	Самостоятельная теоретическая подготовка. Работа с нормативной документацией	2ч.25 мин.	Освоение профессиональных компетенций: ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам; ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности; ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие; ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами; ОК 09. Использовать информационные технологии в профессиональной деятельности; ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках;

				ПК 3.2 Организовывать работу коллектива исполнителей. ПК 3.3 Анализировать результаты деятельности коллектива исполнителей.
2.	Изучение ассортимента выпускаемой продукции и географии поставок ПАО «АМЗ»	Самостоятельная теоретическая подготовка. Работа с нормативной документацией	2ч.25 мин. 2ч.25мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10; ПК 3.2; ПК 3.3
3.	Изучение деятельности отдела информационных технологий ПАО «АМЗ»	Самостоятельная теоретическая подготовка. Работа с нормативной документацией	2ч.25 мин. 2ч.25мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10; ПК 3.2; ПК 3.3
4.	Организация работы отдела ИТ	Самостоятельная теоретическая подготовка. Работа с нормативной документацией	2ч.25 мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10; ПК 3.2; ПК 3.3
5.	Изучение аппаратного и программного обеспечения отдела ИТ	Самостоятельная теоретическая подготовка. Работа с нормативной документацией	2ч.25 мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10; ПК 3.2; ПК 3.3
6.	Изучение работы компьютерной сети	Изучение организации и технологии профессиональной деятельности	2ч.25 мин. 2ч.25мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09;

				ОК 10; ПК 3.2; ПК 3.3
7.	Изучение сетевого оборудования	Изучение организации и технологии профессиональной деятельности	2ч.25 мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10; ПК 3.2; ПК 3.3
8.	Изучение сетевых программных средств и способов сетевого администрирования	Изучение организации и технологии профессиональной деятельности	2ч.25 мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10; ПК 3.2; ПК 3.3
9.	Сетевое взаимодействие между компьютерами локальной сети	Приобретение профессиональных и организаторских навыков	2ч.25 мин. 2ч.25мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10; ПК 3.2; ПК 3.3
10.	Изучение сетевой информационной безопасности	Изучение организации и технологии профессиональной деятельности. Работа с нормативной документацией	2ч.25 мин. 2ч.25мин. 2ч.25мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10; ПК 3.2; ПК 3.3
11.	Изучение комплексной системы защиты информации	Изучение организации и технологии профессиональной деятельности.	2ч.25 мин. 2ч.25мин. 2ч.25мин.	Освоение профессиональных компетенций: ОК 01; ОК 02; ОК 03; ОК 04; ОК 09; ОК 10;

				ПК 3.2; ПК 3.3

Министерство образования, науки и молодежной политики Нижегородской области
Государственное бюджетное профессиональное образовательное учреждение
«Арзамасский коммерческо-технический техникум»

СОГЛАСОВАНО
Руководитель предприятия
(организации)
_____
«__»_____20___ г.
М.П.

УТВЕРЖДАЮ
И.о. зам. директора по УиНМР
_____Н.В. Слюдова
«___»_____20___ г.

ОТЧЕТ
О ПРОХОЖДЕНИИ СТАЖИРОВКИ

преподавателя (мастера производственного обучения)
УД ЕН.03 Информационные технологии в профессиональной деятельности
специальности 13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)

Ванюшиной Ольги Владимировны

Арзамас
2022 г.

1. Наименование программы стажировки Развитие и совершенствование профессиональных компетенций по информационным технологиям
2. Форма стажировки без отрыва от основной работы
3. Срок стажировки 24.02.2022 г. – 25.03.2022 г. в соответствии с приказом по стажировке: №6-лс/к от 24.02.2022 г.
4. Место прохождения стажировки Нижегородская область, г. Арзамас, ул. 9 Мая, д. 2, ПАО «Арзамасский машиностроительный завод»
5. Цель стажировки развитие и совершенствование профессиональных компетенций, изучение передового опыта
6. Руководитель стажировки начальник отдела информационных технологий ПАО «АМЗ» Васильев А.Б.
7. Дневник

Дата	Время	Выполняемая работа
24.02	2ч.25мин.	***ИЗУЧЕНИЕ ХАРАКТЕРИСТИКИ ПРЕДПРИЯТИЯ*** ПАО «Арзамасский машиностроительный завод» является ведущим градообразующим предприятием Арзамаса, а также одним из крупнейших предприятий нижегородской автомобильной промышленности. Доля, выпускаемой предприятием продукции, составляет 30% от всей продукции, выпускаемой промышленными предприятиями города. ПАО «АМЗ» основано в 1972 году как Арзамасский завод автомобильных запасных частей Горьковского объединения по производству автомобилей. Всего за тридцать пять лет завод стал ведущим предприятием РФ по производству бронетехники. На сегодняшний день - это завод со специализацией по выпуску бронетранспортеров БТР-80, БТР-80А, Водник, Тигр, БТР-90 и по изготовлению деталей и узлов к автомобилям, выпускаемых ОАО «ГАЗ». ПАО «АМЗ» занимает площадь 867,9 тыс. кв.м., в том числе производственную 232,0 тыс. кв.м., из нее 177,7 тыс. кв.м. - производственные цеха. В производственную сферу ПАО «АМЗ» входит три основных и два вспомогательных производства. К основным производствам относятся:

		Производство автокомпонентов. Структура производства автокомпонентов представлена сложным комплексом взаимосвязанных цехов завода. Главная задача которых - обеспечить необходимый выпуск автокомпонентов согласно графику поставки. Заводом освоены и выпускаются карданные валы, амортизаторы к грузовым и легковым автомобилям, выхлопные системы и другие детали. В основном эта продукция идет на конвейеры ГАЗа и другие заводы. Объемы механосборочного производства постоянно увеличиваются. К ПА относятся: МСЦ-3, МСЦ-9, цех амортизаторов, цех термообработки и металлопокрытий, цех амортизаторов. В производстве задействовано 1281 единица оборудования. Численность производства 954 человека. ***Производство сборки серийных машин.*** Здесь задействовано 108 единиц оборудования. К ПСМ относятся: МСЦ-5, МСЦ-6. В этих цехах ведется сборка, изготовление и ремонт серийных автомобилей. Общая численность производства составляет 521 человек. ***Производство серийных деталей и узлов.*** Это производство изготавливает узлы и запасные части к серийно выпускаемым автомобилям. Состоит из следующих подразделений: МСЦ-1, МСЦ-2, МСЦ-4, МСЦ-9. В производстве задействовано 1779 единиц оборудования. Численность производства 781 человек. На сегодняшний день ПАО «Арзамасский машиностроительный завод» — это предприятие, находящееся в периметре управления ООО «Военно-промышленная компания» (г. Москва). За 40 лет своего существования Арзамасский машиностроительный завод стал одним из лидеров оборонно-промышленного комплекса страны, единственным предприятием в России по выпуску колесной бронетехники, ведущим предприятием машиностроительной отрасли Нижегородской области. Начиная свою деятельность с производства амортизаторов, он прошел все стадии развития на пути к созданию конечного продукта – передовых образцов мирового рынка вооружения.
25.02 28.02	2ч.25мин. 2ч.25мин.	***ИЗУЧЕНИЕ АССОРТИМЕНТА ВЫПУСКАЕМОЙ ПРОДУКЦИИ И ГЕОГРАФИИ ПОСТАВОК ПАО «АМЗ»*** БТР-80, БТР-80А, БТР-80К, БТР-82/82А, БММ, БРЭМ-К, УНШ, СТС «Тигр» –основной перечень серийно выпускаемой продукции. При этом каждая разработка АМЗ – это принципиально новые возможности и решения, постоянное улучшение основных характеристик. И вместе с тем, все они отвечают предъявляемым к такому роду техники требованиям: надежность, качество, мощь, маневренность. Это делает ее востребованной на мировом рынке и позволяет предприятию быть надежным стратегическим партнером всех силовых структур государства (МО, МВД, ФСБ, ФСО и других ведомств), сотрудничать более чем с 30 странами мира и миротворческими силами ООН. За последнее время география поставок продукции производства ПАО «АМЗ» значительно расширилась. Техника

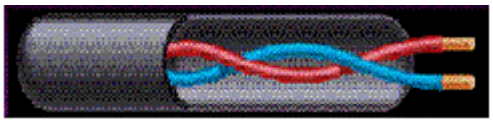
		спецназначения пользуется высокой популярностью у военных Алжира, Венгрии, Индонезии, Судана, Джибути, Вьетнама, Шри-Ланки, Узбекистана, Казахстана, Азербайджана и др. Российские бронемашины производства ПАО «АМЗ» «перешагнули» через океан и завоевывают рынок Латинской Америки (Уругвай, Колумбия). Предприятие ежегодно демонстрирует свою продукцию на крупнейших международных выставках вооружения и военной техники, среди которых международная выставка в Малайзии «Defense Service Asia», парижская «Eurosatory», южноафриканская «Africa Aerospace & Defence», выставка в Объединенных Арабских Эмиратах «Index» и многие другие. Визитной карточкой завода по праву считается БТР-80. Основные отличительные особенности этой машины − это простота эксплуатации, высокая надежность и живучесть. БТР-80 подвижен и обладает мощным двигателем, способен вести бой, даже при подрыве на мине или при повреждении шин пулями. Одновременно с производством и поставкой спецтехники предприятие активно проводит работы, как по модернизации продукции, так и по созданию новой техники (СПМ-3 «Медведь» и гражданский вариант изделия «Тигр»). Помимо поставки военной техники одним из приоритетных направлений деятельности предприятия является неразрывная связь с организациями-потребителями на весь период производимого изделия. Завод осуществляет гарантийное обслуживание техники, проводит доработки, ремонт и модернизацию ранее выпущенной продукции. По решению МО РФ об организации сервисного обслуживания военной техники в войсках силами завода-изготовителя в 2010 году на предприятии создан сервисный центр, специалисты которого осуществляют плановое обслуживание техники, восстановительный ремонт, обучение личного состава эксплуатации и т.п. С 2010 года в рамках выполнения экспортных контрактов на предприятии было освоено новое направление — обучение иностранных специалистов. Ежегодно экспертами «Военного регистра» на ПАО «АМЗ» проводится инспекционный контроль, сертифицированной системы менеджмента качества на соответствие требованиям стандартов ГОСТ РВ 15.002-2003 и ГОСТ Р ИСО 9001-2008. Чётко продуманная кадровая политика, грамотно выстроенная работа с персоналом, профессиональный подход к оплате труда как никогда необходимы в современных условиях, потому как именно это позволяет предприятию сохранять ценные кадры и привлекать высококвалифицированных специалистов. Благодаря этому завод имеет настоящий внутренний стержень, который даёт возможность уверенно смотреть в будущее и строить самые смелые планы.
1.03 2.03	2ч.25мин. 2ч.25мин.	***ИЗУЧЕНИЕ ДЕЯТЕЛЬНОСТИ ОТДЕЛА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПАО «АМЗ»*** Отдел информационных технологий является структурным подразделением ПАО «Арзамасский машиностроительный завод». Отдел в своей деятельности руководствуется Конституцией Российской Федерации, законами Российской Федерации, указами и

		распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, законами и иными нормативными правовыми актами РФ, приказами и распоряжениями директора ПАО «АМЗ» и положением об отделе информационных технологий. Структура и численность отдела определяется штатным расписанием ПАО «АМЗ». Отдел по всем вопросам своей работы подчиняется директору и заместителю, курирующему направление деятельности отдела. ***Основные задачи отдела ИТ*** ● 1. Организационное, информационное и технологическое обеспечение деятельности ПАО «АМЗ» по и сопровождение мероприятий, проводимых им. ● 2. Разработка и проведение политики в сфере внедрения и сопровождения современных информационных технологий. ● 3. Участие в разработке и реализации федеральных и областных программ в сфере внедрения современных информационных технологий. ● 4. Защита и сохранение конфиденциальной информации на электронных носителях, ее рациональное и эффективное использование. ● 5. Обеспечение бесперебойного функционирования аппаратно-программных комплексов. ● 6. Обеспечение требуемого уровня информационной безопасности. Обеспечение парольной защиты. ● 7. Обеспечение информационной и технической поддержки средств вычислительной техники и программного обеспечения. ● 8. Проведение работ по оптимизации использования информационных ресурсов. ● 9. Подготовка нормативных документов по правилам работы с вычислительной техникой и офисным оборудованием. ● 10. Контроль за исполнением нормативных документов по правилам работы с вычислительной техникой и офисным оборудованием. ● 11. Контроль и своевременное исполнение поступающих заявок. ● 12. Обеспечение своевременного резервного копирования данных. ● 13. Обеспечение антивирусной защиты данных. ● 14. Обеспечение техники безопасности. ***Функции отдела ИТ*** Отдел, в соответствии с возложенными на него задачами, осуществляет следующие основные функции: • 1. Организация формирования и развития информационно телекоммуникационной системы, организация обеспечения защиты информации. • 2. Обеспечение функционирования информационно-телекоммуникационной системы, в том числе: • 2.1. администрирование ЛВС, баз данных и прикладных информационных систем обработки информации; • 2.2. администрирование телекоммуникационного узла.

		• 3. Обслуживание электронной и коммуникационной техники, обеспечение исполнения договоров соответствующими организациями, установление взаимодействия с оператором связи и контроль за поставкой услуг связи в соответствии с требованиями предприятия. • 4. Обеспечение процессов сбора, хранения, предоставления информации с использованием прикладных информационных систем. • 5. Обеспечение и поддержка системы защиты информации. • 6. Настройка и поддержка средств разграничения доступа к базам данных; антивирусных средств при обмене и вводе информации. • 7. Организация контрольных проверок на объектах обработки сведений, составляющих государственную тайну. • 8. Разработка технологии решения задач по всем этапам обработки информации. • 9. Выполнение работы по подготовке программ к настройке. • 10. Разработка инструкций по работе с программами, оформление необходимой технической документации. • 11. Сопровождения и внедрение программ и программных средств. • 12. Обобщение, изучение и анализ передового опыта в области развития современных информационных технологий. • 13. Организация работы по соблюдению стандартов современных информационных технологий. • 14. Отслеживание новостей и тенденций развития информационных, информационно-вычислительных и автоматизированных систем и сетей, программных средств, баз и банков данных. • 15. Разработка, внедрение и организация контроля исполнения руководящих документов по обеспечению информационной безопасности. • 16. Разработка и внедрение инструкций, регламентов и стандартов использования программного и аппаратного обеспечения. Своевременное рассмотрение и исполнение заявок, связанных с функционированием программного и аппаратного обеспечения. ***Полномочия отдела ИТ*** ● 1. Запрашивать и получать в установленном порядке от подразделений необходимую для осуществления своей деятельности. ● 2. Взаимодействовать с органами государственной власти, органами местного самоуправления, предприятиями и учреждениями по вопросам, входящим в компетенцию отдела. ● 3. Использовать государственные системы связи и телекоммуникаций. ● 4. Планировать в установленном порядке командировки сотрудников отдела. ● 5. Готовить предложения по модификации и осуществлять модификацию аппаратно-программных комплексов с целью повышения эффективности их использования.

		● 6. Проводить проверки использования средств вычислительной техники, внутренних и внешних информационных ресурсов. ● 7. Вносить предложения о применении административных мер во всех случаях нарушений подразделениями и должностными лицами установленных правил работы с вычислительной техникой и информационными ресурсами. ● 8. Пресекать случаи нецелевого использования внутренних и внешних информационных ресурсов доступными средствами в установленном порядке.
3.03	2ч.25мин.	***ОРГАНИЗАЦИЯ РАБОТЫ ОТДЕЛА ИТ*** ● 1. Работой отдела руководит начальник отдела, который утверждается на должность директором ПАО «АМЗ» и освобождается от нее его приказом и входит в основную номенклатуру должностей. ● 2. Работники отдела назначаются на должность и освобождаются от нее директором ПАО «АМЗ» по представлению руководителя отдела. ● 3. Отдел прекращает свою деятельность в связи с его упразднением (ликвидацией) или реорганизацией. ● 4. Начальник отдела: ● 4.1. Руководит деятельностью отдела и несет персональную ответственность за качественное и своевременное выполнение задач и функций, возложенных на отдел в соответствии с настоящим положением. ● 4.2. Распределяет обязанности между сотрудниками отдела. ● 4.3. Представляет в установленном порядке сотрудников отдела к поощрению и к взысканию. ● 4.4. Отвечает за служебную дисциплину сотрудников отдела. ● 2. Должностные обязанности сотрудников отдела определяются должностными инструкциями, утверждаемыми директором ПАО «АМЗ». ● 3. Для эффективной и рациональной работы отдела составляется ежемесячный план работы отдела. Каждый работник отдела контролирует выполнение мероприятий плана, за выполнение которых он отвечает. ● 4. Общий контроль за выполнением всего ежемесячного плана работы отдела осуществляет начальник отдела. ● 5. Ответственность за невыполнение плана работы при отсутствии объективных причин несет начальник отдела, а на период его отсутствия - заместитель начальника отдела. Заместитель начальника отдела осуществляет техническое руководство работой отдела в отсутствие начальника отдела.
4.03	2ч.25мин.	***СОДЕРЖАНИЕ И ФОРМЫ ДЕЯТЕЛЬНОСТИ ОТДЕЛА ИТ*** При выполнении задачи проектирования организационных, технических и экономических решений по применению информационных технологий отдел выполняет следующие работы:

		1. Собирает информацию о возможностях различного оборудования и программного обеспечения. Оценивает применимость различного оборудования и программного обеспечения для достижения поставленных целей. 2. Собирает информацию о рыночных ценах на необходимое оборудование, услуги и программное обеспечение, о возможных поставщиках и подрядчиках и дает предварительную оценку стоимости реализации и эксплуатации проекта. 3. При сотрудничестве с другими подразделениями, разрабатывает организационно-технические требования и документы, описывающие и регламентирующие методы реализации и эксплуатации проекта, а также взаимодействие между подразделениями при реализации проектов 4. Поиск, сбор, анализ и обработка информации по новым информационным, технологическим, экономическим и управленческим технологиям в Интернете и иных источниках, для нужд отдела и предприятия.
9.03	2ч.25мин.	***ИЗУЧЕНИЕ АППАРАТНОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТДЕЛА ИТ*** Отдел информационных технологий располагает достаточным техническим парком для комфортной и бесперебойной работы. Все компьютеры, расположенные в отделе, объединены в локальную сеть и соединены с другим оборудованием, необходимым для работы. Это позволяет обеспечить быстрый обмен данными, удобство работы. В отделе ИТ используются персональные компьютеры со следующими аппаратными характеристиками: ● Процессоры: Intel Core i3 CPU 3220 3.30 GHz, Intel Core 2 Duo CPU E6750 2.66 GHz, Intel Corei3 CPU 530 2.90 GHz и Intel Corei5 CPU 3570 3.40 GHz. ● ОЗУ: 4,00 ГБ и 8,00 Гб. ● Видеокарты: GPU Nvidia Geforce GT 740, Nvidia Geforce GT 8600, GPU Nvidia Geforce GT 650TI. Серверы: ● Процессор: семейство процессоров Intel Xeon E-2300, процессор Intel Pentium. ● ОЗУ: 8 ГБ - 128 ГБ, UDIMM (DDR4). ● Контроллер LAN: встроенный Intel i210 2 порта Ethernet 10/100/1000 Мбит / с (ускорение TCP / IP). ● Графика: 1 x VGA (15-контактный) / дополнительно 1 x VGA на передней панели (не для базового блока 10 x 2,5 дюйма). На персональных компьютерах отдела ИТ установлено следующее программное обеспечение: ● ОС MS Windows 7. ● Пакет программ Microsoft Office. ● ОС MS Windows Server 2012 R2. ● Microsoft SQL Server. ● Пакет программ 1С. ● ABBYY FineReader. Антивирусная защита обеспечивается приложениями Dr.Web Антивирус, Kaspersky Security.
10.03	2ч.25мин.	***ИЗУЧЕНИЕ РАБОТЫ КОМПЬЮТЕРНОЙ СЕТИ***

11.03	2ч.25мин.	Для выполнения своих функций сотрудникам отдела ИТ необходим выход в Internet и наличие электронной почты. Вся информация, используемая в работе, хранится в БД на сервере. Для организации процесса работы отдела все компьютеры объединены в локальную сеть. Таким образом, к общим системным ресурсам относятся: - файл-сервер; - сервер БД; - Proxy сервер. Локальная сеть представляет собой совокупность сервера и АРМ. В качестве топологии локальной сети выбрана топология «звезда». Выбор обусловлен простотой добавления новых абонентов в сеть, так как в перспективе предполагается рост структурного подразделения, а, следовательно, и расширение сети. При построении сети по топологии «звезда» отказ одного из абонентов не заметен, что является ещё одним плюсом, так как сотрудники в отделе работают сравнительно независимо, и в случае необходимости один из абонентов может взять на себя функции другого. Топология «звезда» предполагает, что все абоненты, подключённые к сети, могут передавать данные одновременно, однако коммутатор абонент может производить обмен данными только с одним абонентом. Данные, передаваемые одной станцией, доступны только станции получателя сети. Поэтому следует учесть, что при выходе из строя коммутатора, который является общим связующим звеном для всех составляющих локальной сети, влечёт за собой недоступность передаваемого ресурса для всех ее составляющих. ***Кабельная подсистема сети*** Кабельная система - система телекоммуникационных кабелей, проводников, шнуров и пассивного коммутационного оборудования, поддерживающая коммутацию информационного технологического оборудования. Для организации локальной сети был выбран кабель типа неэкранированная витая пара категории 5E, который изображён на рисунке 1.  Рисунок 1. Неэкранированная витая пара Выбор обусловлен такими преимуществами как доступность инструментов для установки разъёмов (RJ45), удобство прокладки кабеля (гибкий), относительная простота ремонта при повреждении. Кабель UTP категории 5E обеспечивает поддержку перспективных высокоскоростных сетей. Между рабочими станциями локальной сети кабель прокладывается не прямо (непосредственно), а, проходя через ряд устройств сети - хабы, кроссы, заканчивается розеткой. Подобная кабельная сеть называется структурированной. Если в дальнейшем будут перемещения персонала внутри здания из одних помещений в другие, проводку не нужно будет изменять: достаточно аппаратуру

		из одних помещений перенести в другие и сделать необходимые переключения на кроссировочных панелях. На каждое рабочее место устанавливается не менее двух четырехпарных розеток RJ-45. Каждая из них отдельным кабелем категории 5E соединяется с патч-панелью, установленной в специальном помещении. Патч-панель, или панель соединений, представляет собой группу розеток RJ-45, смонтированных на пластине шириной 19 дюймов. Это стандартный размер для универсальных коммуникационных шкафов - рэков (rack), в которых устанавливается оборудование (концентраторы, серверы, источники бесперебойного питания и т.п.). На обратной стороне панели смонтированы соединители, в которые монтируются кабели. Унифицированная проводка применяется для передачи всех видов сигналов - голоса, данных, видео, мультимедиа и графики. От розетки до компьютера идёт гибкий кабель, называемый «патч-корд» («patch-cord»). От розеток по коробам жесткий кабель идёт к кросс-панели. К кросс-панели кабель прикрепляется жёстко («врезается») сзади. Кросс-панель, в свою очередь, крепится к стене. Рядом с кросс панелью расположен сетевой коммутатор. На передней стенке кросс-панели есть пронумерованные выходы, разъёмы, число которых соответствует количеству гнёзд сзади. Кросс-панель соединена с сетевым коммутатором посредством небольших гибких участков кабеля, патч-кордов. Конечным пунктом прокладки всех кабелей является то место, где укреплена кросс-панель, то есть телекоммуникационный шкаф. Для защиты кабельной системы от механических повреждений кабель помещается в специальные короба, куда обычно закладываются и кабели электропитания оборудования. Таким образом, полученная кабельная система состоит из трех подсистем: - Подсистема рабочего места. Эта подсистема предназначена для подключения устройств потребителей: компьютеров, терминалов, принтеров и т.п. к локальной сети. - Горизонтальная подсистема. Она проложена неэкранированными витыми парами. - Подсистема управления. Состоит из панелей с множеством разъемов, соединительных кабелей или шнуров, обеспечивающих переключение цепей. К основным характеристикам кабельной системы относится ее универсальность, так как в подобной кабельной системе могут функционировать практически все типы локальных сетей, и порты проводки полностью взаимозаменяемы и переключаются механически в подсистеме управления. Второй ее особенностью является избыточность. Это означает, что при проектировании предусмотрены подводы к дополнительным рабочим местам, лёгкость замены электронного оборудования и другие эксплуатационные преимущества. Структурированная кабельная система, построенная на основе витой пары категории 5E, имеет очень большую гибкость в использовании.
14.03	2ч.25мин.	***ИЗУЧЕНИЕ СЕТЕВОГО ОБОРУДОВАНИЯ*** Выбор сетевого оборудования является одной из важнейших задач проектирования сети. В качестве сервера необходимо использовать компьютер с достаточно высокой производительностью, большим

		объемом оперативной памяти и жестких дисков, быстродействующим сетевым адаптером. В данном случае монитор, устройства ввода (клавиатура, мышь) могут быть самыми простыми, так как сервер не предусматривается использовать в качестве рабочего компьютера. При выборе рабочих станций стоит акцентировать внимание на быстродействии процессоров и большом объёме оперативной памяти. Так же для создания комфортных условий работы сотрудников организации следует выбрать качественные мониторы, которые обладают минимальным негативным воздействием на здоровье человека. Для защиты от перебоев в системе питания необходимо предусмотреть наличие источника бесперебойного питания, который при сбое питания переходит на питание подключенного компьютера от аккумулятора и подаёт специальный сигнал компьютеру, который за короткое время завершает все текущие операции и сохраняет данные на диске. При выборе источника главными характеристиками, на которые следует обращать внимание - это максимальная мощность, которую он обеспечивает, и время поддержания им номинального уровня напряжения. Важное место в локальной вычислительной сети занимает коммутационный шкаф. Непосредственного участия в работе сети шкаф не принимает, его главной функцией является защита активного и пассивного оборудования, которое в него устанавливается, от пыли, электромагнитных полей, изменения температуры и механических воздействий. Для обеспечения безопасности информации, хранящейся на сервере, и ограничения доступ к нему посторонних лиц сервер следует установить в запираемый телекоммуникационный шкаф. В качестве соединения с сетью Internet выбрано ADSL соединение. Технология ADSL позволяет передавать аналоговые сигналы обычной телефонной связи по той же паре телефонных проводов, которая используется для передачи потока данных. На обоих концах линии аналоговые сигналы отфильтровываются от цифрового высокочастотного сигнала, позволяя использовать обычную телефонную связь одновременно с передачей данных. Для реализации соединения с глобальной вычислительной сетью необходим ADSL модем и телефонная линия.
15.03	2ч.25мин.	***ИЗУЧЕНИЕ СЕТЕВЫХ ПРОГРАММНЫХ СРЕДСТВ И СПОСОБОВ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ*** Для управления локальной сетью, ее администрирования, выделен отдельный специалист - администратор, который будет иметь всю информацию о конфигурации сети, распределении ресурсов и следить за корректным использованием сети всеми пользователями. В обязанности администратора входит: - создание групп пользователей различного назначения; - определение прав доступа пользователей; - обучение новых пользователей и оперативная помощь в случае необходимости; - контроль дискового пространства сервера сети; - защита и резервное копирование данных, борьба с компьютерными вирусами;

		- модернизация программного обеспечения и сетевой аппаратуры; - настройка сети для получения максимальной производительности. В данной сети применяется следующее программное обеспечение: - сетевая многозадачная операционная система, установленная на сервере обработки (серверный вариант); - операционная система, установленная на всех автоматизированных рабочих местах (вариант для рабочих станций); - ПО стека протоколов TCP/IP; - ПО поддержки сетевой СУБД; - ПО автоматизированной обработки информации. В качестве операционной системы, которая установлена на сервере, выбран продукт компании Microsoft - Windows Server 2012. Выбор обусловлен необходимостью обеспечения безопасности ресурсов сети. Windows Server 2012 использует ряд механизмов для обеспечения безопасности локального компьютера от злоумышленных программ, идентификации пользователей и обеспечения безопасности передачи данных по сети. Основные механизмы безопасности Windows Server 2012 перечислены ниже. В их числе: - тотальный контроль за доступом, предотвращает подключение ненадёжных компьютеров к безопасным системам при помощи фильтрации пакетов и трансляции сетевых адресов, гарантируя, что разрешённые сеансы пользователей не могут быть сфальсифицированы, украдены или мистифицированы, и предотвращает нарушение программой адресного пространства другой программы при помощи защиты памяти; - определение личности пользователя при помощи методов аутентификации; - запрет или разрешение доступа на основе личности пользователя, при помощи списков контроля доступа для объектов с управляемой безопасностью посредствам шифрования файлов, путём ограничения доступа к возможностям операционной системы, которые могут быть использованы неправильно, при помощи групповой политики и путём авторизации удалённых пользователей, подключённых через Интернет или удалённое соединение; - запись деятельности пользователя посредством журналов аудита особенно значимой информации и журналов соединений для публичных служб, таких как Web и FTP; - минимизация риска неправильной конфигурации путём группировки похожих механизмов безопасности в политики и последующего применения этих политик к группам похожих пользователей или компьютеров. На всех рабочих станциях, подключённых к серверу, целесообразно установить операционную систему Windows 2007. В качестве программного обеспечения сетевой СУБД выбран сервис MS SQL Server 2016, работающий под управлением операционной системы Windows Server 2012. В качестве программного обеспечения автоматизированной обработки информации в локальной сети установлена программа «1С бухгалтерия».
16.03 17.03	2ч.25мин. 2ч.25мин.	***СЕТЕВОЕ ВЗАИМОДЕЙСТВИЕ МЕЖДУ КОМПЬЮТЕРАМИ ЛОКАЛЬНОЙ СЕТИ***

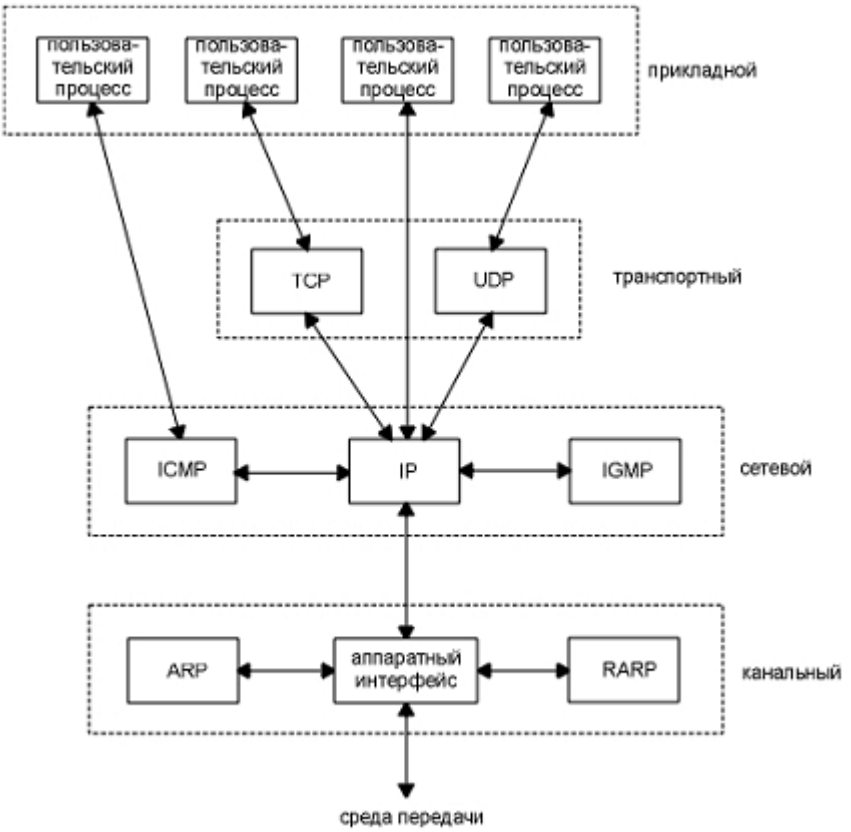
Семейство протоколов TCP/IP объединяет практически любые компьютеры и обеспечивает сетевое взаимодействие между компьютерами. Сетевые протоколы разработаны по уровням, причем каждый уровень отвечает за собственную фазу коммуникаций. Семейство протоколов TCP/IP - это комбинации различных протоколов на различных уровнях. TCP/IP состоит из четырех уровней, как показано на рисунке 2.

Рисунок 2. Четыре уровня протоколов TCP/IP

Каждый уровень несет собственную функциональную нагрузку. Канальный уровень или уровень сетевого интерфейса включает в себя драйвер устройства в операционной системе и соответствующую сетевую интерфейсную плату в компьютере. Вместе они обеспечивают аппаратную поддержку физического соединения с сетью (с кабелем). Сетевой уровень, иногда называемый уровнем межсетевого взаимодействия, отвечает за передачу пакетов по сети. Маршрутизация пакетов осуществляется именно на этом уровне. Транспортный уровень отвечает за передачу потока данных между двумя компьютерами и обеспечивает работу прикладного уровня, который находится выше. Прикладной уровень определяет детали каждого конкретного приложения.

На рисунке 3 показано взаимодействие протоколов различных уровней и UDP - два основных протокола транспортного уровня. Оба используют IP в качестве сетевого уровня, который осуществляет надежную передачу данных между двумя компьютерами. Он обеспечивает деление данных, передающихся от одного приложения к другому, на пакеты подходящего для сетевого уровня размера, подтверждение принятых пакетов, установку тайм-аутов, в течение которых должно прийти подтверждение на пакет, и так далее, отправляет и принимает датаграммы (datagram) от одного компьютера к другому. Датаграмма - это блок информации (определенное количество байт информации, которое указывается отправителем), который отправляется от отправителя к приемнику. С точки зрения безопасности, в отличие от TCP, UDP является ненадежным протоколом. Не существует гарантий, что датаграмма достигнет конечной точки назначения. За надежность передачи данных при использовании датаграмм отвечает прикладной уровень - это основной протокол сетевого уровня. Он используется как TCP, так и UDP. Каждый блок информации TCP и UDP, который

		передается по объединённым сетям, проходит через IP уровень в каждой конечной системе и в каждом промежуточном маршрутизаторе. На рисунке 3 показаны приложения, которые имеют прямой доступ к IP. С точки зрения безопасности IP ненадёжный протокол, предоставляющий сервис доставки датаграмм без соединения, то есть не существует гарантии того, что IP датаграмма успешно достигнет пункта назначения. IP не подтверждает доставку данных и не контролирует целостность полученных данных. Однако IP предоставляет определённый сервис обработки некоторых событий. Когда, например, возникает ситуация временного переполнения буфера у маршрутизатора, IP применяет простой алгоритм обработки ошибок: он отбрасывает датаграмму и старается послать ICMP сообщение отправителю. Следовательно, любая требуемая надёжность должна быть обеспечена верхними уровнями (например, TCP), является дополнением к протоколу IP. Он используется IP уровнем для обмена сообщениями об ошибках и другой жизненно важной информацией уровня IP. Несмотря на то, что ICMP используется в основном IP уровнем, приложения также могут получить доступ к ICMP. Протокол управления группами Internet (IGMP - Internet Groupe Management Protocol), используется при групповой адресации: при этом UDP датаграммы рассылаются нескольким получателям. Протокол определения адреса (ARP - Address Resolutio№Protocol) и обратный протокол определения адреса (RARP - Reverse Address Resolutio№Protocol) это специализированные протоколы, используемые только с определённым типом сетевых интерфейсов. Они применяются для преобразования формата адресов, используемого IP уровнем в формат адресов, используемый сетевым интерфейсом.

		 Рисунок 3. Различные протоколы на разных уровнях семейства протоколов TCP/IP
18.03 21.03 22.03	2ч.25мин. 2ч.25мин. 2ч.25мин.	***ИЗУЧЕНИЕ СЕТЕВОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*** Профессиональная деятельность специалистов отдела ИТ ПАО «АМЗ» в сфере иформационной безопасности регламентируется международным стандартом ГОСТ Р ИСО/МЭК 15408-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Настоящий стандарт устанавливает структуру и содержание компонентов функциональных требований безопасности для оценки безопасности. Он также включает каталог функциональных компонентов, отвечающих общим требованиям к функциональным возможностям безопасности многих продуктов и систем ИТ. Мероприятия, необходимые для обеспечения безопасности информации, обрабатываемой в ЛВС ПАО «АМЗ» включают в себя: 1. Защита данных от потерь в сетях является централизованное копирование данных на высокопроизводительном стримере большой емкости, подключенном к серверу с использованием интерфейса SCSI. В такой схеме представлены следующие основные компоненты: клиент системы резервного копирования и сервера. Клиент системы резервного копирования - компьютерная система, данные из которой подлежат резервному копированию. Система в данном случае должна быть представлена файловым сервером, сервером приложений и баз данных, а также программным компонентом, который считывает данные из устройств хранения и отправляет их на сервер резервного копирования. Такое программное

		обеспечение обычно поставляется в комплекте систем резервного копирования. Серверы резервного копирования - системы, которые копируют данные и регистрируют выполненные операции. Технологически сервера резервного копирования делятся на два типа: Master- сервер и Media - сервер. Master-сервер - сервер управления системой резервного копирования. В его задачу входит планирование операций резервного копирования и восстановления, а также ведения каталога резервных копий. Программный компонент сервера управления резервным копированием, выполняющий функции, менеджера резервного копирования. Media - сервер - сервер копирования резервируемых данных. Его основной задачей является выполнение команд поступающих от Master-сервера, по копированию данных. К серверам данного типа подключаются устройства хранения резервных копий. Устройство хранения резервных копий - накопители на лентах, магнитных или оптических дисках. Процедура создания резервных копий представляется собой трехстороннее взаимодействие между клиентом, Master-сервером и Media-сервером. Клиент отправляет список файлов, подлежащих резервному копированию, на Master- сервер, а данные со своих томов на Media-сервер. В свою очередь менеджер резервного копирования инициирует и контролирует выполнение заданий в соответствии с заданным расписанием. Media-сервер выбирает одно или несколько устройств хранения, загружает носители информации, принимает от клиента по сети и записывает их на носители резервных копий. Аналогичным образом только в обратном направлении происходит восстановление данных из резервных копий. 2. Брандмауэры целесообразно расположить на стыках сети Интернет и DMZ, DMZ и внутренней сети. Во втором случае будет использоваться встроенный сетевой экран системы Windows Server плюс настроенные списки разграничения ACL маршрутизатора, который должен быть настроен по запретительному принципу - администратор задает только те параметры (адреса, протоколы, порты, службы, бюджеты пользователей и т. д.), функционирование которых разрешено, все остальные службы запрещены, в первом - аппаратный межсетевой экран. Для выбора такого экрана необходимо учитывать следующие требования: - это должно быть решение от известного производителя; - должно присутствовать достаточное количество портов Fast Ethernet; - осуществление контроля на прикладном уровне с учетом состояния, контроля прикладного протокола; - проверка пакетов на соответствие заданным условиям; - поддержка Exchange; - обнаружение и предотвращение несанкционированного доступа; - высокая производительность. 3. Выбор конкретной антивирусной программы зависит от многих факторов (стоимость, результаты тестирований и др.), к числу которых относится и его популярность. К примеру, доли основных участников рынка антивирусной защиты в России на 2021 год распределились следующим образом (рисунок 4).

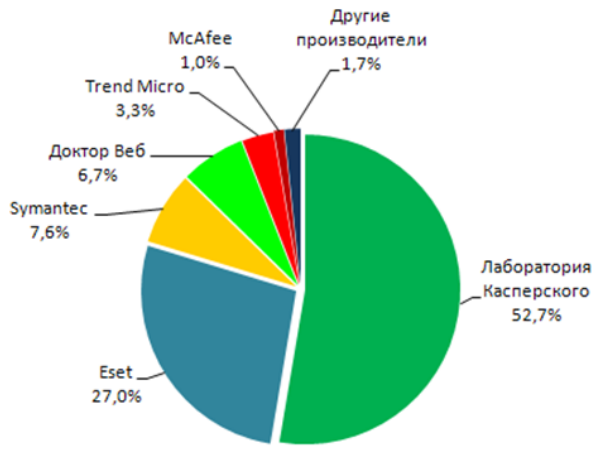


Рисунок 4. Распределение рынка антивирусных компаний

Задача обеспечения антивирусной защиты корпоративной сети - одна из первоочередных задач в процессе построения комплексной защиты ЛВС.

При выборе антивирусных программ необходимо учитывать результаты независимых тестирований.

После анализа состава компонентов антивирусных пакетов данной фирмы, очевидно, что для использования в корпоративной локальной сети наиболее подходит Kaspersky Security Center - решение для целостной зашиты корпоративных сетей от всех видов современных интернет-угроз.

4. Контроль программ, устройств и Веб-Контроль.

Централизованное управление IT-инфраструктурой позволяет создать политики безопасности и обеспечить дополнительную защиту ценных данных, Можно устанавливать правила для групп и отдельных пользователей. Ограничивать запуск нежелательных приложений в сети с помощью Контроля программ. Создавать правила доступа для устройств, которые пользователи подключают к сети, на основании типа или серийного номера устройства, а также на основании способа подключения устройства. Отслеживать и контролировать доступ в интернет для всего предприятия или групп пользователей.

5. Средства системного администрирования.

Помимо детального контроля над обеспечением безопасности IT-инфраструктуры, Kaspersky Security Center предоставляет средства системного администрирования, которые упрощают задачи управления инфраструктурой и позволяют повысить производительность и сократить операционные издержки.

Развертывание ОС и программ Kaspersky Security Center дает возможность управлять образами ОС и программ: создавать, оперативно копировать и развертывать.

6. Мониторинг уязвимостей.

После инвентаризации аппаратного и программного обеспечения можно выполнить поиск уязвимостей в операционных системах и приложениях, для которых не были установлены исправления:

- формирование подробных отчетов об уязвимостях;

		- выполнение оценки уязвимостей и расставление приоритетов для установки исправлений. Обнаружив уязвимости, можно эффективно организовать распространение самых важных исправлений с помощью Kaspersky Security Center: - управление загрузкой исправлений с серверов «Лаборатории Касперского»; - управление установкой обновлений и исправлений Microsoft на компьютеры сети. 7. Для обеспечения управляемости и безопасности сети также необходимо обеспечить разграничение полномочий доступа пользователей к достаточно большому количеству сетевых ресурсов. Традиционным решением этого вопроса является создание доменов сети. Домен есть одно из основных средств формирования пространства имён каталога Active Directory (АД). Наряду с доменами таковыми средствами формирования являются административная иерархия и физическая структура сети. В настоящее время используются три основных способа построения АД и создания доменов: - создание в ЛВС одного домена, обслуживающего всю сеть в целом - целесообразно применять при относительно небольшом размере фирмы и отсутствии ее разделения на отдельные подразделения; - создание леса доменов с глобальным каталогом (или корнем леса), в роли которого выступает основной домен - применяется при географическом разнесении отделов фирмы. В этом случае свои домены существуют у головного офиса фирмы и ее филиалов, связаны они через сеть Интернет; - создание некоторого количества независимых доменов с глобальным каталогом - применяется при жестком административном разделении фирмы на несколько отделов. Таким образом, вариант построения АД и домена зависит, прежде всего, от административной модели предприятия. Основой домена станет сервер с установленной серверной операционной системой MS Windows Server 2012 - основной контроллер домена (PDC). Путем создания доменной структуры решаются следующие задачи: - создание областей административной ответственности - возможно деление корпоративной сети на области, управляемые отдельно друг от друга; - создание областей действия политики учетных записей - политика учетных записей определяет правила применения пользователями учетных записей и сопоставленных им паролей. В частности задается длина пароля, количество неудачных попыток ввода пароля до блокировки учетной записи, а также продолжительность подобной блокировки; - разграничение доступа к объектам - каждый домен реализует собственные настройки безопасности (включая идентификаторы безопасности и списки контроля доступа); - изоляция трафика репликации - для размещения информации об объектах корпоративной сети используются доменные разделы каталога. Каждому домену соответствует свой раздел каталога, называемый доменным. Все объекты, относящиеся к некоторому

		домену, помещаются в соответствующий раздел каталога. Изменения, произведенные в доменном разделе, реплицируются исключительно в пределах домена; - ограничение размера копии каталога - каждый домен Active Directory может содержать до миллиона различных объектов. Тем не менее, реально использовать домены такого размера непрактично. Следствием большого размера домена является большой размер копии каталога. Соответственно, огромной оказывается нагрузка на серверы, являющиеся носителями подобной копии. В целом создание доменной структуры сети позволит упростить и автоматизировать администрирование сети, повысить ее управляемость, масштабируемость и безопасность. Основной контроллер домена содержит копию АД, которая описывает всю ЛВС и политики взаимодействия между ее элементами. Такая информация является исключительно важной для функционирования всей сети, при ее потере ЛВС превращается просто в совокупность рабочих станций, серверов, другого оборудования и утрачивает возможность исполнять свои функции. Поэтому необходимо предусмотреть создание резервного контроллера домена сети (BDC) - копии основного и работающего параллельно с ним. Наличие резервного контроллера домена оправдано и в других случаях, к примеру, обновления аппаратного обеспечения основного сервера.
23.03 24.03 25.03	2ч.25мин. 2ч.25мин. 2ч.25мин.	***ИЗУЧЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ*** Необходимо также защищать информацию, которая циркулирует внутри предприятия. Это достигается за счёт: 1. Дополнительной идентификации пользователей; 2. Защиты внутреннего трафика в сети ПАО «АМЗ». Для осуществления вышеуказанных мероприятий применяется система комплексной защиты информации «Панцирь». Она решает следующие задачи: - реализация разграничительной политики внешнего доступа к ресурсам локальной вычислительной сети; - реализация разграничительной политики доступа к ресурсам в корпоративной ПС, в локальной, либо в распределенной корпоративной сети; - шифрование трафика в локальной вычислительной сети; - ключи eToken PRO/32K и eToken PRO/64K (в форм факторе USB ключа и смарт-карты); - криптопровайдер «КриптоПро CSP», сертифицирован по требованиям к шифрованию конфиденциальной информации ФСБ России. - СЗИ содержит в своем составе следующие компоненты: Клиентскую часть. Устанавливается на компьютеры в составе ЛВС. Реализует прозрачное для пользователя шифрование трафика на стеке протоколов TCP/IP и разграничительную политику доступа субъектов к объектам. - Криптопровайдер «КриптоПро CSP» - применяется при необходимости использования сертифицированного по требованиям

		безопасности решения. Устанавливается вместе с клиентской частью на компьютеры в составе корпоративной сети и на серверную часть. - Серверную часть (основную). Устанавливается на выделенном компьютере в составе корпоративной сети. Идентифицирует компьютеры в составе корпоративной сети, автоматически генерирует и предоставляет клиентским частям сеансовые ключи шифрования, формирует разграничительную политику доступа к ресурсам, осуществляет аудит идентификации субъектов и объектов доступа в корпоративной сети. - АРМ администратора безопасности. Устанавливается на выделенном компьютере в составе корпоративной сети. Предоставляет администратору безопасности интерфейс настройки VPN, инструментальные средства обработки аудита. В СЗИ «Панцирь» для идентификации субъектов и объектов доступа введена отдельная логическая сущность «Идентификатор субъекта/объекта» (ID), которая, в общем случае, никак не связана ни с конкретным компьютером, ни с учетной записью пользователей, заведенных на компьютере. При создании на сервере VPN субъекта/объекта доступа администратор безопасности создает его идентификатор, и, в соответствии с тем, что эта сущность идентифицирует (пользователя или компьютер) размещает данный идентификатор при установке клиентской части СЗИ в соответствующем ресурсе компьютера (объект реестра или файловый объект) для его последующей идентификации, либо предоставляет данный идентификатор на внешнем носителе пользователю (Flash-устройство, электронный ключ или смарт-карта). Данная сущность не является секретной информацией, передается по каналам связи в открытом виде, служит для идентификации субъекта/объекта на сервере VPN и взаимной идентификации субъектов/объектов в составе корпоративной VPN. При назначении идентификатора субъекту/объекту на сервере VPN администратор безопасности относит его либо к корпоративным, либо к доверенным (присваивая идентификатору соответствующую дополнительную логическую сущность «тип субъекта/объекта»). Корпоративные субъекты/объекты смогут взаимодействовать только с корпоративными субъектами/объектами (на которых устанавливаются клиентские части СЗИ), весь трафик между ними будет шифроваться). Доверенные субъекты/объекты смогут взаимодействовать, как с корпоративными субъектами/объектами (на которых устанавливаются клиентские части СЗИ), весь трафик между ними будет шифроваться, так и с внешними по отношению к корпоративной VPN субъектами/объектами по открытым каналам связи. Решение по реализации ключевой политики в СЗИ основано на использовании двух типов симметричных ключей шифрования: ключ шифрования трафика между клиентской и серверной частями (технологический ключ) и сеансовые ключи шифрования между парами клиентских частей.

		При создании субъекта/объекта доступа на сервере VPN, вместе с назначением идентификатора и его типа (корпоративный или доверенный), администратором безопасности генерируется технологический ключ (для каждого субъекта/объекта генерируется свой технологический ключ). В зависимости от того, что представляет собою сущность субъект/объект (пользователя или компьютер), администратор размещает технологический ключ при установке клиентской части СЗИ в ресурсе компьютера (объект реестра или файловый объект), либо предоставляет технологический ключ на внешнем носителе пользователю (Flash- устройство, электронный ключ или смарт-карта), на этом же носителе должен располагаться идентификатор пользователя Технологический ключ является секретной информацией, возможность несанкционированного доступа к которой должна предотвращаться, ключ не должен передаваться по каналу связи в открытом виде. Технологический ключ используется для получения в зашифрованном виде клиентской частью VPN таблицы сеансовых ключей субъекта/объекта для обмена информацией с другими субъектами/объектами из состава VPN (для каждой пары субъектов/объектов свой сеансовый ключ), и при сеансовой идентификации субъекта/объекта на сервере VPN при запросе таблицы сеансовых ключей. Сеансовая идентификация субъекта/объекта на сервере VPN осуществляется следующим образом. Клиентская часть СЗИ автоматически при включении компьютера, если идентифицируется субъект/объект компьютер, либо по запросу пользователя - при подключении пользователем к компьютеру носителя с идентифицирующей его информацией - ID и технологическим ключом шифрования, если идентифицируется субъект/объект пользователь, обращается к серверу VPN, высылая ему в открытом виде соответствующий идентификатор (ID) и хэш (необратимое шифрование) технологического ключа. Сервер VPN, получив запрос от субъекта/объекта, определяет его ID, определяет корректность соответствия технологического ключа и ID. Если они соответствуют, сеансовая идентификация субъекта/ объекта считается успешной (об этом, и в случае некорректной идентификации, на сервере VPN откладывается соответствующая информация в аудите). В СЗИ реализовано три иерархических уровня реализации разграничительной политики доступа к ресурсам корпоративной VPN. Первый уровень - уровень контроля доступа к сетевым ресурсам. Состоит в полном запрете доступа к сетевым ресурсам не идентифицированных субъектов/объектов. Реализуется следующим образом. Вне зависимости от того, как определен субъект/объект доступа, на котором установлена клиентская часть СЗИ, кроме, как к серверу VPN, до осуществления его успешной идентификации на сервере VPN (что подтверждается загрузкой с сервера таблицы сеансовых ключей шифрования), невозможен. Второй уровень - уровень контроля доступа к корпоративным ресурсам. Состоит в реализации различных возможностей доступа к сетевым ресурсам для корпоративных и доверенных

		субъектов/объектов. Корпоративным субъектам/объектам разрешается взаимодействие только с корпоративными субъектами/объектами, при этом их трафик шифруется соответствующими сеансовыми ключами (для каждой пары субъект/объект свой сеансовый ключ шифрования). Доверенным субъектам/объектам разрешается взаимодействие, как с корпоративными субъектами/объектами, при этом их трафик шифруется соответствующими сеансовыми ключами (для каждой пары субъект/объект свой сеансовый ключ шифрования), так и с внешними по отношению к корпорации субъектами/объектами, при этом их трафик не шифруется. Это реализуется следующим образом. При сетевом взаимодействии в рамках VPN, взаимодействующие клиентские части взаимно идентифицируют друг друга (обмениваются своими ID). Результатом подобной взаимной идентификации является принятие сторонами решения о возможности взаимодействия, при возможности - выбор способа взаимодействия, при выборе защищенного способа - выбор сеансового ключа шифрования. Так, если к корпоративному субъекту/объекту обращается корпоративный субъект/объект, будет осуществлена взаимная идентификация субъектов/объектов клиентскими частями СЗИ, взаимодействие сторонам будет разрешено, каждой стороной будет однозначно определен сеансовый ключ шифрования (он свой для каждой пары идентифицированных субъектов/объектов). То же произойдет, если к доверенному субъекту/объекту обращается доверенный субъект/объект (их взаимодействие будет разрешено по защищенному сеансовым ключом каналу). В случае если к корпоративному субъекту/объекту обращается некий внешний по отношению к VPN субъект/объект, не будет осуществлена взаимная идентификация субъектов/объектов взаимодействие будет запрещено. В случае если к доверенному субъекту/объекту обращается некий внешний по отношению к VPN субъект/объект, не будет осуществлена взаимная идентификация субъектов/объектов - взаимодействие будет разрешено по открытому каналу связи. То же произойдет и в случае, если доверенный субъект/объект обращается к некому внешнему по отношению к VPN субъекту/объекту. Третий уровень - уровень разграничения доступа к корпоративным ресурсам в составе VPN. К корпоративным ресурсам VPN имеют доступ корпоративные и доверенные субъекты/объекты (доступ к ним осуществляется по защищенным сеансовыми ключами каналам связи), каждый из которых идентифицируется своим ID. Реализация разграничений доступа состоит в возможности задания администратором безопасности (разграничительная политика реализуется с сервера VPN) разграничений (разрешений или запретов) по взаимодействию корпоративных и доверенных субъектов/объектов между собою - задается какой ID с каким ID может (либо не может) взаимодействовать. При задании разграничительной политики доступа к корпоративным ресурсам на сервере VPN, после успешной идентификации субъекта/объекта на сервере, с сервера ему будет передана таблица сеансовых ключей шифрования (и идентификаторов субъектов/объектов) только тех субъектов/объектов, с которыми разрешено взаимодействие

		идентифицированному субъекту/объекту в рамках реализации заданной разграничительной политики доступа к ресурсам VPN. Идентифицировавшийся субъект/объект сможет взаимодействовать только с теми субъектами/объектами VPN, для взаимодействия с которыми им будут получены с сервера VPN сеансовые ключи шифрования. Таким образом, для функционирования данной системы в АО «Арзамасский машиностроительный завод» установлены сервер VPN, серверная часть системы, а также клиентские части. Для рассматриваемой локальной вычислительной сети система безопасности состоит из следующих элементов: - Разграничение доступа к ресурсам (парольное, служба AD); - Разграничение доступа к ресурсам с помощью e-Toking (в составе КСЗИ «Панцирь»); - Размещение внутренних сегментов сети в демилитаризованной зоне; - Использование брандмауэров; - Использование системы резервного копирования и источников бесперебойного питания; - Использование антивирусного программного обеспечения; - Шифрование внутрисетевого трафика (КСЗИ «Панцирь»). Применение данного комплекса мер позволяет надёжно обезопасить обрабатываемую в локальной вычислительно сети информацию от атак из сети Интернет и внутренних атак.

3. Краткое описание практической значимости стажировки для использования в учебном процессе
   Практическая значимость стажировки заключается в том, что собран теоретический и практический материал по теме: Развитие и совершенствование профессиональных компетенций по виду профессиональной деятельности «Информационные технологии в профессиональной деятельности», который может быть использован в учебном процессе. Рассмотрены теоретические и практические аспекты организации работы компьютерной сети и сетевой информационной безопасности, которые представляют большой интерес в практике преподавания информационных дисциплин.
4. Отчет о прохождении стажировки рассмотрен на заседании методического объединения_____
   Протокол заседания от_____ №_____
5. Заключение руководителя стажировки от организации
   За время стажировки Ванюшина Ольга Владимировна освоила программу стажировки в объеме 72 часа с соблюдением плана-графика. Проявила самостоятельность при выполнении должностных обязанностей и исполнительность в работе. Компетентно отражены профессиональные аспекты деятельности отдела ИТ ПАО «АМЗ» в сфере организации работы компьютерной сети и её информационной безопасности. Информация, содержащаяся в отчёте о стажировке, собрана в соответствии с паспортом программы.

Руководитель стажировки _____
_____

подпись *ФИО*

М.П.

6. Заключение руководителя стажировки от техникума (председатель МО)

Во время прохождения стажировки Ванюшина О.В. собрала материал, обобщающий основные аспекты организации деятельности структурного подразделения ПАО «АМЗ». Собранный материал представляет собой отличную базовую информацию для проведения практических работ, связанных с телекоммуникационными технологиями. Изучение теоретических аспектов работы, общение со специалистами в сфере IT-технологий значительно обогащает преподавателя информацией, необходимой для организации учебного процесса в рамках учебной дисциплины ЕН.03 «Информационные технологии в профессиональной деятельности».

Руководитель стажировки
(председатель МО) _____ Богомолова Н.И.

подпись *ФИО*

Стажёр _____/О.В. Ванюшина/

СПРАВКА

Выдана Ванюшиной О.В.
преподавателю ГБПОУ «Арзамасский коммерческо-технический техникум»
в том, что она с «24» февраля 2022 г. по «25» марта 2022 г. прошла стажировку на предприятии ПАО «Арзамасский машиностроительный завод»
по теме: Развитие и совершенствование профессиональных компетенций по информационным технологиям специальности 13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)
в объеме_____72 часа_____

Выполняемые стажёром работы: согласно программе стажировке

- *Самостоятельную теоретическую подготовку;*
- *Приобретение профессиональных и организаторских навыков;*

- *Изучение организации и технологии профессиональной деятельности;*
- *Непосредственное участие в планировании работы предприятия, цеха, участка, отдела;*
- *Работу с нормативной и другой документацией;*
- *Выполнение функциональных обязанностей должностных лиц (в качестве временно исполняющего обязанности или дублера);*
- *Участие в совещаниях, деловых встречах и др.*

Прохождение стажировки признано успешным.

Дата выдачи «___»_____20_____ г.

М.П.

Руководитель организации_____/_____