Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

ЭЛЕКТРОННЫЕ ИНСТРУКЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СОТРУДНИКОВ ПРЕДПРИЯТИЯ

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 555

Екатеринбург 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____ И. А. Суслова
«____» _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ЭЛЕКТРОННЫЕ ИНСТРУКЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СОТРУДНИКОВ ПРЕДПРИЯТИЯ

Исполнитель:
обучающаяся группы № ЗИБ-501 Д. С Милютина
Руководитель:
кандидат педагогических наук,
доцент А. А. Шайдуров
Нормоконтролер: С. Ю. Ярина

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из набора электронных инструкций и пояснительной записки на 60 страницах, содержащей 13 рисунков, 23 источников литературы.

Ключевые слова: ИНСТРУКЦИЯ, ЗАЩИТА ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Милютина Д. С., Электронные инструкции по информационной безопасности для сотрудников предприятия**:** выпускная квалификационная работа / Д. С. Милютина; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2017. — 52 с.

В работе рассмотрены проблемы соблюдения политики информационной безопасности ООО «Global Truck Sales».

Цель работы — разработать набор электронных инструкций по курсу «Информационная безопасность и защита информации» для использования в процессе обучения сотрудников ООО «Global Truck Sales». Для достижения цели был проведен анализ предприятия, существующих регламентов и инструкций. На основе сотрудничества с заказчиком было создано набор электронных инструкций, размещенное на внутреннем обучающем ресурсе компании.

С учетом тенденций высокого спроса на информацию, необходимо постоянно контролировать знания сотрудников в этой сфере, а также контролировать соблюдение установленных норм.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы разработки политики информационной безопасности обусловлена тем, что в наше время ни одна организация не обходится без обмена данными в сети Интернет, с каждым годом увеличивается количество информации, растет ее ценность, а следовательно, растет необходимость в защите информации. Эти данные подвержены риску, особенно, это касается конфиденциальной информации. Для того, чтобы максимально защитить информацию возникает необходимость комплексного подхода.

Актуальность проблемы так же обусловлена постоянно меняющимися угрозами информации, технический прогресс не стоит на месте и с каждым днем появляются все новые угрозы, вирусы и пути обхода, политика информационной безопасности должна предвосхитить возможные уязвимости без вреда для компании и обезопасить бизнес от возможных финансовых потерь.

«Общепринято понимать под политикой информационной безопасности документ, в котором отражены основные направления, цели и задачи, свои обязательства и важнейшие принципы деятельности предприятия в области защиты информации, официально сформулированные высшим руководством и принятые к обязательному выполнению на предприятии» [7].До недавнего времени необходимость в разработке политики информационной безопасности в основном определялась пониманием руководства организации проблемы защиты ресурсов компьютерных систем и сетей организации. Надо сказать, что на российском рынке сложился рынок услуг по разработке документов такого рода, однако весьма различающихся по составу и содержанию.

Объект исследования — обучение сотрудников предприятия ООО «Global Truck Sales» основным знаниям Политики информационной безопасности согласно инструкциям Политики информационной безопасности.

Предметом исследования являются типовые инструкции по информационной безопасности, адаптированные под исследуемую организацию.

Цель работы — разработать набор электронных инструкций по курсу «Информационная безопасность и защита информации» для использования в процессе обучения сотрудников ООО «Global Truck Sales».

Задачи исследования:

- проанализировать общую характеристику объекта защиты в организации;
- проанализировать степень защищенности объектов защиты по каждому из видов защиты информации (ЗИ) (правовая ЗИ, организационная ЗИ, программно-аппаратная ЗИ, инженерно-физическая ЗИ);
- внести свои предложения по защите информации;
- разработать набор электронных инструкций для обучения сотрудников основам информационной безопасности.

Методы исследования: изучение и анализ литературы, наблюдение, разработка и апробация набора электронных инструкций.

Во введении обоснована актуальность выбора темы, поставлена цель и задачи анализа, охарактеризованы методы исследования и источники информации.

Глава первая представляет собой анализ печатных и интернет-источников по созданию Политики информационной безопасности. В главе второй подробно рассмотрена структура предприятия, используемые меры безопасности и предосторожности. Глава имеет практический характер, в ней предлагаются новые методы защиты для улучшения состояния информационной безопасности на предприятии. Третья глава описывает основы электронных инструкций, общие требования к их разработке и описание разработанного продукта. В заключении делаются выводы о проделанной работе, а также подводятся итоги выполнения поставленных задач.

1 НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

1.1 Обзор печатных и интернет-источников по настройке политики безопасности в различных организациях

1.1.1 Обзор печатных изданий по настройке политики безопасности в различных организациях

Сергей Петренко в книге «Политика безопасности компании при работе в Интернет» [13] предлагает в первую очередь опираться на международные стандарты и выделяет распределение доступа по степени доверия к сотрудникам. Однако, автор является приверженцем индивидуального подхода в зависимости от масштаба и функций компании.

В журнале «Молодой ученый» автор Дмитрий Дронов [5] рекомендует начать разработку политики информационной безопасности с анализа возможных угроз: «Для разработки политики безопасности предприятия данного типа необходимо определиться с набором возможных угроз и местом их реализации. В ходе исследования для решения данной задачи использовался классификатор ГОСТ Р 51275—2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». Построение дерева актуальных угроз выполнялось методом экспертного опроса».

Александр Марков [11] в книге «Методы оценки несоответствия средств защиты информации» утверждает: «В общем случае можно выделить следующие процессы, связанные с разработкой и реализацией политики безопасности (ПБ) и поддающиеся автоматизации:

1. Комплекс мероприятий, связанных с проведением анализа рисков. К этой группе можно отнести:

- учет материальных или информационных ценностей;
- моделирование угроз информационной безопасности (ИБ) системы;
- анализ рисков с использованием того или иного подхода — например, стоимостный анализ рисков.

2. Мероприятия по оценке соответствия мер по обеспечению ИБ системы некоторому эталонному образцу: стандарту, формальной политике безопасности, профилю защиты и т. п.

3. Действия, связанные с разработкой разного рода документов, в частности отчетов, диаграмм, профилей защиты, заданий по безопасности.

4. Действия, связанные со сбором, хранением и обработкой статистики по событиям безопасности для организации.

В настоящее время на рынке отсутствуют системы, которые предоставляли бы исчерпывающие средства для автоматизации всех перечисленных аспектов разработки ПБ. Наиболее широко представлены средства для автоматизации анализа рисков, а также для проверки соответствия информационной системы компании положениям того или иного стандарта. Именно на последних системах в силу их относительной новизны, а также с учетом роли, которую они потенциально могут сыграть для популяризации соответствующих стандартов, стоит остановиться подробнее [6].

1.1.2 Обзор интернет-источников

Дмитрий Дудко в своей статье в интернет-журнале «itsec.ru» [6] утверждает, что: «В идеале политика информационной безопасности должна охватывать всю организацию, дочерние предприятия, филиалы и подразделения. Если это по каким-то причинам невозможно, то в Политике информационной безопасности (ПИБ) необходимо предусмотреть раздел по контролю непротиворечивости ПИБ различных элементов организации».

Алексей Дорожкин и Владимир Ясенев [12] отмечают, что концепция обеспечения информационной безопасности предприятия для поддержания экономической безопасности предприятия определяет потенциальные источники угроз информационной безопасности предприятия и меры противодействия им со стороны предприятия и, рассматривая информацию как объект защиты, устанавливает цель и задачи, которые необходимо решить для обеспечения информационной безопасности предприятия.

Развитие современного общества напрямую связано с ростом производства, потребления и накопления информации во всех отраслях человеческой деятельности. Информационные потоки в обществе увеличиваются с каждым днем, и этот процесс носит лавинообразный характер. По своему значению для развития общества информация приравнивается к важнейшим ресурсам наряду с сырьем и энергией. В развитых странах большинство работающих заняты не в сфере производства, а в той или иной степени занимаются обработкой информации. Вместе с тем можно отметить и новую тенденцию, заключающуюся во все большей информационной зависимости общества в целом и отдельного человека в частности. Именно поэтому в последнее время появились такие категории, как «информационная политика», «информационная безопасность», «информационная война» и целый ряд других новых понятий, в той или иной мере связанных с информацией. Столь же ярко демонстрирует повышение роли информации в производственных процессах появление в XX в. такого понятия, как промышленный шпионаж. Не материальные ценности, а чистая информация становится объектом хищения. Это обстоятельство подчеркивает, насколько важной является информация для современного общества. Информационная безопасность является одной из главных проблем, с которой сталкивается современное общество. Причиной обострения этой проблемы является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации [1].

Однако следует отметить, что снижение рисков для компании не должно сказываться на удобстве работы пользователей. Как показывает практика, большинство пользователей халатно относится к безопасности информации и хранению данных, из этого следует, что одна из главных задач политики информационной безопасности — регламентация условий хранения и передачи данных, для сохранения конфиденциальности, защиты от изменения информационных ресурсов.

Политика безопасности затрагивает все субъекты информационных отношений в организации, поэтому на этапе разработки политики безопасности очень важно разграничить их права и обязанности, связанные с их непосредственной деятельностью.

С позиции обеспечения информационной безопасности разграничение прав и обязанностей целесообразно провести по следующим группам (функционалу):

- специалист по информационной безопасности/системный администратор;
- владелец информации;
- поставщики аппаратного и программного обеспечения;
- руководители отделов;
- менеджеры отделов;
- аудиторы.

Таким образом, благодаря разработанной Политике безопасности обществу с ограниченной ответственностью (ООО) «Global Truck Sales» удастся защитить данные от утери и кражи, предупредить действия злоумышленников или конкурентов и обезопасить данные от утечки информации.

Основной задачей политики информационной безопасности является минимизация рисков потери данных и утечки информации. Политика информационной безопасности представляет собой совокупность мер и регламентов по защите данных. Политика должна быть утверждена высшим руководством компании (совет директоров, генеральный директор). Кроме того, с

Политикой информационной безопасности должны быть ознакомлены все сотрудники, имеющие доступ к автоматизированному рабочему месту.

1.1.3 Обзор законодательной базы

Наиболее явно требования к документальному определению вопросов информационной безопасности указаны для предприятий, выпускающих оборонную продукцию — в ГОСТ 15.002-2000, где предусматривается обязательная программа обеспечения безопасности как часть политики качества. Указанный документ должен включать совокупность процедур, мероприятий и процессов обеспечения безопасности разработки (производства) средств защиты информации (СЗИ) (составляющей государственную тайну), согласуется с представителем заказчика и подлежит обязательному инспекционному контролю. Однако определение и требования к содержанию собственно Политики информационной безопасности. Однако, определение и требования к содержанию собственно Политики безопасности даны во вступившем в силу с 2004 года ГОСТ 15408-02 и международном стандарте ISO 17799» [2].

Федеральные законы, к которым рекомендуют обращаться авторы изученной литературы при разработке Политики информационной безопасности:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ [19].

Данный федеральный закон определяет порядок по применению информационных технологий и обеспечению данных информационной безопасности, предусматривает права и обязанности граждан РФ, владеющих информацией, а также запреты на пропагандирование и распространение отдельных видов информации.

2. Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ, описывает принципы и условия обработки персональных данных, права субъекта персональных данных, обязанности оператора сбора персо-

нальных данных, меры для обеспечения безопасности персональных данных, государственный контроль и надзор за обработкой персональных данных и ответственность за нарушения.

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях (введена Федеральным законом от 25.07.2011 г. № 261-ФЗ).

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона.

Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов [18].

Федеральный закон от 06.04.2011 г. «Об электронной подписи» № 63-ФЗ перечисляет области деятельности, в которых может быть использована электронная подпись, регламентирует средства электронной подписи, содержит требования к аккредитованным удостоверяющим центрам.

Исходя из вышеописанного становится ясно, что разработка политики информационной безопасности предприятия должна начинаться в первую очередь с постановки целей и конкретных их формулировок, а также определения объема составляемого документа. Основная цель такого документа как, Политика информационной безопасности — установление базиса для всех остальных документов регламентирующих действия пользователей в том числе тех, в которых рассказывается почему необходимо защищать информацию.

Мнения экспертов едины в одном — разработка ПИБ начинается с анализа рисков конкретного предприятия, ведь у каждой сферы бизнеса индивидуальные особенности, в каждом регионе свои опасности, поэтому при разработке ПИБ необходимо учитывать не только сферу бизнеса, а индивидуальные особенности сотрудников, территориального расположения предприятия, конкурентов и недоброжелателей. Кроме того, разработчику так же необходимо учесть общую подготовку линейного персонала, руководителей, директората компании.

Особое внимание стоит уделить и техническому оснащению организации, многие руководители экономят на оборудовании, что напрямую может увеличить риск угрозы утечки информации, таким образом, на плечи разработчика ПИБ ложится аналитика оборудования, и то, как в текущих реалиях улучшить качество оборудования, либо предусмотреть риски связанные с техническим оснащением регламентировав основные положения использования оборудования и доступа к нему.

Еще одним важным аспектом является документационное обеспечение соблюдения положений ПИБ. Таким образом, работодатель распределяет ответственность между сотрудниками и может обезопасить себя от утечки информации в данном звене уже на законодательном уровне.

Немалое внимание при разработке ПИБ уделяется и физической безопасности объекта. Физическая безопасность представляет собой организа-

цию доступа на объект, пропускного режима, контроль доступа к данным и их сохранности.

Еще одним важным принципом разработки ПИБ является единство. Правила должны быть едины для всех, будь то сотрудники, или филиалы компании, в каждом отделе и в каждом дочернем предприятии действует одна общая Политика информационной безопасности.

Наиболее нерадивыми пользователями информации является линейный персонал, в т.ч. линейные руководители, опираясь именно на эту группу пользователей необходимо уделить наибольшее внимание при разграничении информации на категории доступа, разрешению и согласованию доступа к информации и составлению регламентов на просмотр, удаление и изменение информационных ресурсов.

Перед разработчиком стоит большая задача, в которой необходимо учесть не только требования заказчика, но и большой спектр рисков различной сложности и опасности, ведь говоря о политике информационной безопасности организации нельзя ограничиваться только технической составляющей. Большого внимания требует и физическая безопасность как организации в целом, так и каждого ее субъекта, кроме того, разработчик должен предусмотреть процессы подбора кадров, документооборота, хранения ресурсов доступных сотрудникам.

После проведения оценки рисков, составления плана мероприятий по их исключению, авторы рекомендуют разработчику помимо учета информационных ценностей, так же провести учет материальных ценностей компании, составить общую картину финансовых ущербов всех рисков.

1.2 Характеристика предприятия «Global Truck Sales»

1.2.1 Описание предприятия

Объектом обследования является предприятие ООО «Global Truck Sales». Компания «Global Truck Sales» (Глобал Трак Сейлс) занимается продажей грузовой техники европейского и российского производства и является зарекомендованным торговым партнером компании GTS (Global Truck Service) — сети сервисных станций по ремонту и обслуживанию импортной грузовой автотехники.

Компания «Global Truck Sales» работает на российском рынке уже более 15 лет, и на сегодняшний день устойчиво занимает одну из лидирующих позиций в сфере продаж грузовой техники. На протяжении многих лет начиная с 2006 года сеть «Global Truck Service» занимала первое место по обороту запчастей среди сервисных станций Volvo в России.

Сеть «Global Truck Sales» включает в себя сеть офисов в ряде крупных городов. Линейка услуг и товаров «Global Truck Sales» регулярно обновляется. Компания оперативно реагирует на рыночные и законодательные изменения и формирует свое предложение таким образом, чтобы клиенты «Global Truck Sales» могли пользоваться только передовыми технологиями в соответствии с законом.

ООО «Global Truck Sales» работает по принципу «магазин-склад», когда практически вся техника доступна к отгрузке в день оплаты и находится в наличии на собственной стоянке. Концепция презентации техники состоит в том, что тягачи и полуприцепы новые и с пробегом перед покупкой можно осмотреть, потрогать, и протестировать. Это означает, что разработчику Политики информационной безопасности необходимо уделить внимание регламентированию доступа на стоянку техники, для защиты от угона.

Клиенты «Global Truck Sales» — это физические и юридические лица, работающие на рынке грузоперевозок. С первой сделки сотрудники «Global

Truck Sales» ориентируются на сотрудничество с клиентами-партнерами, которое включает в себя послепродажное обслуживание, различные схемы обмена и выкупа техники, систему скидок и особых условий при покупке каждой следующей единицы.

Основными поставщиками новой техники являются заводы-изготовители или их представительства, дистрибьюторы.

Компания «Global Truck Sales» является дилером российских и европейских производителей полуприцепов и постоянно расширяет ассортимент техники, чтобы удовлетворить потребности самых взыскательных клиентов.

Поставщиками техники с пробегом являются:

- крупные европейские и российские транспортные компании, обладающие большими парками грузовой техники;
- малые и средние транспортные компании, частные перевозчики, индивидуальные предприниматели (ИП);
- банки и лизинговые компании;
- официальные представители и дилеры заводов-изготовителей, продающие технику по схеме trade-in;
- европейские и российские партнеры, занимающиеся продажами грузовой техники;
- средние и крупные европейские перевозчики, а также европейские компании, занимающиеся сдачей техники в аренду, имеющие многотысячные флоты;
- клиенты, ранее приобретавшие технику в Компании (комиссия, trade-in).

Географическое расположение объекта представлено на рисунке 1.

Рисунок 1 — Географическое положение объекта

Юридический адрес компании: 115035 г. Москва, Овчинниковская наб., д. 22/24, с. 1, помещение 36.

Фактический адрес: Екатеринбург, ул. Черняховского, 92.

Основным видом деятельности компании является: виды деятельности (кроме производства и предоставления аренды), связанные с торговлей, ремонтом и техническим обслуживанием автомобилей и мотоциклов, включая грузовики и большегрузные платформы (фуры), такие как оптовая торговля и розничная торговля новыми и бывшими в употреблении названными транспортными средствами, их ремонт и техническое обслуживание, продажу запчастей для транспортных средств и мотоциклов.

Вспомогательные виды деятельности:

- деятельность агентов, действующих на основании договоров комиссии, участвующих в оптовой торговле и продаже транспортных средств;
- мытье, полировку транспортных средств и т.д.

1.2.2 Организационная структура предприятия

Ценностями компании ООО «Global Truck Sales» являются:

- лояльность: сохранение низкой стоимости товаров и услуг;
- качество: быстрое и качественное предоставление услуг;
- клиентоориентированность: любовь своих клиентов и стараемся максимально быстро решать их проблемы.

Организационная структура предприятия, сформирована с целью обеспечения достижения целей компании и построена по функциональному управлению. Здесь имеет место вертикаль: Генеральный директор — руководители отделов — исполнители. Организация осуществляет свою деятельность в соответствии с действующим законодательством Российской Федерации и Уставом предприятия.

Организационная структура регулирует разделение задач по отделам и подразделениям; их компетентность в решении определенных проблем, общее взаимодействие между сотрудниками всех отделов.

Организационная структура компании ООО «Global Truck Sales» представлена на рисунке 2.

Рисунок 2 — Организационная структура «Global Truck Sales»

1.2.3 Служба по вопросам защиты информации

Конкретная служба по защите информации на предприятии ООО «Global Truck Sales» отсутствует. Ответственность за защищаемую информацию несет генеральный директор, директора офисов, служба безопасности компании и IT-специалисты на местах. За информацию, относящуюся к коммерческой тайне, несут ответственность все служащие предприятия.

1.2.4 Анализ и характеристика информационных ресурсов предприятия

Исследуемое предприятие содержит следующие информационные ресурсы:

Информация, относящаяся к коммерческой тайне:

- заработная плата;
- договоры с юридическими и физическими лицами;
- технологии и технические средства;
- личные данные клиентов;
- личные данные сотрудников;
- данные о ценообразовании;
- финансовые данные объекта.

Защищаемая информация:

- личные дела сотрудников;
- трудовые договора;
- личные карты сотрудников;
- правила внутреннего распорядка сотрудников;
- должностные обязанности руководителей; специалистов и служащих;

- инструкции пользователей информационно-вычислительных сетей и баз данных;
- памятка сотрудника о сохранении коммерческой или иной тайны;
- содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности;
- прочие разработки и документы для внутреннего пользования.

Открытая информация:

- буклеты;
- информация на web-сайте организации;
- учредительный документ;
- устав;
- цены на товары и услуги.

При приеме на работу каждый сотрудник должен ознакомится с должностными обязанностями и правилами внутреннего распорядка и поставить подпись об ознакомлении на бланке подписей в каждой инструкции.

1.2.5 Угрозы информационной безопасности характерные для «Global Truck Sales»

На предприятии существует угрозы доступности, целостности и конфиденциальности информации.

Угрозами доступности информации являются:

- разрушение (уничтожение) информации, такие как: вирус, повреждение оборудования, чрезвычайная ситуация (например, пожар);
- отказ поддерживающей инфраструктуры: нарушение работы систем связи, электроэнергии, теплоснабжения, кондиционирования, повреждение помещения.

Мерами предотвращения данных угроз являются:

- установка программы антивируса;

- осуществление резервного копирования данных на внешний сервер для быстрого восстановления утерянных данных во время системной ошибки.

Рекомендованные меры предотвращения угроз:

- установка аварийных источников бесперебойного питания;
- подвод электроэнергии не менее чем от двух независимых линий электропередачи;
- плановое обслуживание зданий и в целом всей поддерживающей инфраструктуры.

На момент исследования, в компании на регулярной основе не применялись рекомендованные меры обеспечения безопасности. Обслуживание зданий и поддерживающей инфраструктуры проводилось в соответствии с законодательной базой РФ по пожарной безопасности и в соответствии с требованиями охраны труда. На сегодняшний день, установлен трехфазный источник бесперебойного питания «Power-Vision HF», мощностью 10-60 кВА, со встроенными аккумуляторами. Директорами филиалов и IT-специалистами, совместно с ответственными по пожарной безопасности и охране труда разрабатывается регламент плановой проверки зданий.

Угрозами целостности информации являются:

- нарушение целостности со стороны персонала: ввод неверных данных, несанкционированная модификация информации, кража информации, дублирование данных;
- потеря информации на внешних носителях;
- угрозы целостности баз данных;
- угрозы целостности программных механизмов работы предприятия.

Мерами предотвращения данных угроз может являться следующее:

- введение и смена паролей не реже 1 раза в квартал;

- использование криптографических средств защиты информации (шифрование электронных писем, шифрование конфиденциальных данных сотрудников и бухгалтерии).

Угрозами конфиденциальности являются:

- кражи оборудования;
- делегирование лишних или неиспользуемых полномочий на носитель с конфиденциальной информацией;
- злоупотребления полномочиями доступа к персональным данным клиентов линейными сотрудниками.

Все вышеперечисленные угрозы в настоящее время не были отмечены Службой безопасности компании, так как сотрудники Службы безопасности ведут проверку кандидатов на этапе трудоустройства.

Анализ состояния информационной безопасности на предприятии позволяет выявить следующие угрозы:

1. Ошибки штатных сотрудников, т.е. неверный ввод данных или изменение данных.
2. Внутренний отказ информационной системы, т.е. отказ программного или аппаратного обеспечения, повреждение аппаратуры.
3. Несанкционированный доступ к информации (использование ресурсов без предварительно полученного разрешения). При этом могут совершаться следующие действия: несанкционированное чтение информации, несанкционированное изменение информации, а также несанкционированное уничтожение информации.
4. Кража программно-аппаратных средств и т.д.

1.2.6 Методы и средства защиты информации на предприятии

Защита информации на предприятии осуществляется комплексно и включает в себя меры следующих уровней:

1. Законодательный уровень защиты информации — это законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации ограниченного доступа, а также вводятся меры ответственности за нарушения этих правил.

Режим защиты информации устанавливается:

1. В отношении сведений, отнесенных к государственной тайне, уполномоченными органами на основании Закона Российской Федерации «О государственной тайне».

2. В отношении конфиденциальной документированной информации собственник информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона.

3. В отношении персональных данных — Федеральным законом РФ «Об информации, информатизации и защите информации» от 20.02.1995 г. № 24-ФЗ (ст.21).

В сфере защиты информации ООО «GLOBAL TRUCK SALES» руководствуется следующими нормативно-правовыми актами:

1. Федеральный закон РФ «Об информации, информатизации и защите информации» от 20.02.1995 г. № 24-ФЗ (ст. 21).

2. Закон Российской Федерации «О государственной тайне» (с изменениями от 27 марта 1996 года), принят Верховным Советом Российской Федерации 21.07.1993 г.

3. Закон Российской Федерации «Об информации, информатизации и защите информации», принят Государственной думой 25.01.1995 г.

4. Постановление Правительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.1991 г.

5. Указ Президента Российской Федерации «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использова-

ния специальных технических средств, предназначенных для негласного получения информации» от 09.01.1996 г.

6. Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных», принят Верховным Советом РФ 23.09.1992 г.

7. Закон Российской Федерации «О правовой охране топологий интегральных микросхем», принят Верховным Советом РФ 23.09.1992 г.

2. Административный уровень информационной безопасности.

Как показывает практика последнего времени, различные по масштабам, последствиям и значимости виды преступлений и правонарушений так или иначе связаны с конкретными действиями сотрудников данной организации. Современный опыт показывает, что безопасность деятельности предприятия во многом зависит от того, в какой степени квалификация и обученность ее сотрудников, их морально-нравственные качества соответствуют решаемым задачам.

В связи с этим в целях повышения безопасности ООО «Global Truck Sales» уделяет большое внимание подбору и изучению кадров. Служба безопасности компании проводит проверку сотрудников после согласования кандидатуры на трудоустройство. При этом инструктажи и учения по правилам и мерам безопасности, тестирования сотрудников по постоянно обновляемым программам не проводятся.

В трудовых договорах ООО «Global Truck Sales» очерчивает персональные функциональные обязанности всех категорий сотрудников и на основе существующего российского законодательства во внутренних приказах и распоряжениях определяется их ответственность за любые виды нарушений, связанных с разглашением или утечкой информации, составляющей коммерческую тайну.

3. Организационный уровень защиты информации.

Это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или суще-

ственно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз [21]. Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации компании.

Организационная защита выполняет функции по:

- организации охраны, режима, работу с кадрами, с документами;
- использованию технических средств безопасности и информационно-аналитической деятельности по выявлению внутренних и внешних угроз.

Организационный элемент средств защиты информации включает:

- организацию режима и охраны посредством частного охранного предприятия в круглосуточном режиме, для исключения возможности тайного проникновения на территорию и в помещения посторонних лиц; организация и поддержание надежного пропускного режима и контроля сотрудников, и посетителей;
- организацию работы с сотрудниками по обучению правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации, размещение памяток о соответствии информационной безопасности в служебных помещениях;
- организацию работы с документами, включая разработки и использование документов и носителей КИ, их учет, исполнение, возврат, хранение и уничтожение;
- организацию использования технических средств сбора, обработки, накопления и хранения КИ;
- регламентация разрешительной системы разграничения доступа персонала к защищаемой информации;
- организация ведения всех видов аналитической работы;
- регламентация действий персонала в экстремальных ситуациях;

- регламентация организационных вопросов защиты персональных компьютеров, информационных систем, локальных сетей;
- организация защиты информации — создание службы информационной безопасности или назначение ответственных сотрудников за защиту информации.

Естественно, организационные мероприятия должны четко планироваться, направляться и осуществляться службой информационной безопасности, в состав которой входят специалисты по безопасности.

Таким образом, организационная защита является основным элементом комплексной СЗИ и во многом от того, каким образом реализован организационный элемент, зависит безопасности организации.

В компании ООО «Global Truck Sales» пропускной режим представлен при входе на стоянку, однако офис выполнен в формате Open Space и является зоной доступной для клиентов.

Таким образом, политика информационной безопасности должна быть составлена с учетом всех рисков доступности информации во всех зонах.

1.2.7 Схема сети предприятия

Сведения об аппаратных ресурсах.

Конфигурация ПК (усредненные характеристики клиентских и серверных машин):

Конфигурация клиентских ПК:

- процессоры: Intel core i3, i5;
- оперативная память: 4 / 8 Gb RAM;
- жесткие диск: 500 / 1000 Gb HDD;
- блок питания: 500W.

Конфигурация серверного оборудования:

- процессоры: Intel Xeon e3-1220 v2 / e3-1230 v3 / e5 1410 v2;
- оперативная память: 16/32/64 Gb ECC;

- жесткие диски: 2x300 Gb SAS RAID 0 / 2x3 tb SATA RAID 1 / 2×500 Gb SSD;
- RAID-контроллер: h710 RAID 0/1 hard cache 512 Mb;
- корпус: 1u / 2u / 4u.

Клиентских ПК более 20, серверов 2.

Сведения об операционных системах:

Типы клиентских ОС: Windows 8, Windows 10.

Типы серверных ОС: Windows Server 2012.

На клиентских ПК установлены корпоративные лицензионные версии ПО.

Используемые технологии подключения к сети Ethernet.

Подключение к сети с использованием 4-жильной/8-жильной витой пары (100 или 1000 Мбит/с), все ПК подключаются в управляемые L2 коммутаторы SNR-S2965T-24T / SNR-S2965T-48T.

Для обеспечения физической безопасности объектов применяются системы, видеонаблюдения, охранные сигнализации, а также фактическое присутствие охраны.

В сети используются IPv4 / IPv6 протоколы. Внутренняя пропускная способность сети более 40 Гбит/с, внешние каналы связи более 30 Гбит/с. Используемый тип соединения: Статический IP (IPv4).

Используемая на сети топология: Звезда (главный узел, от которого подключаются все зависимые узлы, но данный тип топологии имеет недостаток, так как в случае недоступности главного узла будут недоступны и все

зависимые узлы).

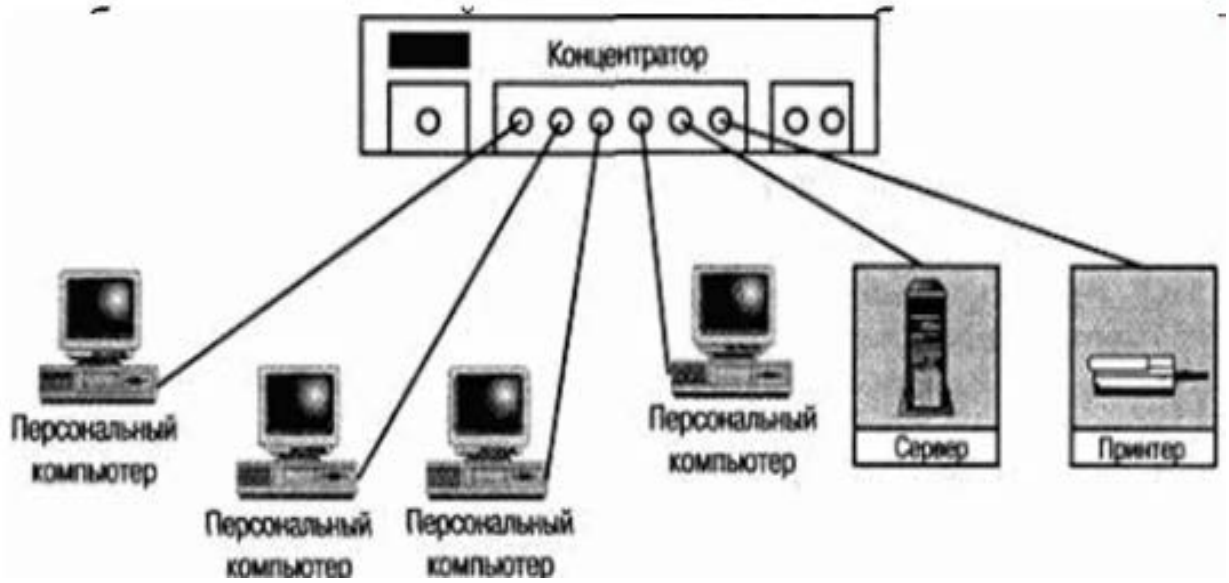


Рисунок 3 — Схема сети на предприятии Global Truck Sales

1.2.8 Программно-аппаратные методы защиты информации

Программно-технические меры защиты информации — это совокупность аппаратных и программных средств и мероприятий по их использованию в интересах защиты конфиденциальности информации.

На предприятии управление доступом путем деления информации по соответствующим должностям и полномочиям осуществляется только при доступе к CRM-системе, расположенной на удаленном рабочем столе (RDP), доступ к системе Windows непосредственно на клиентских ПК не регламентирован, т.е. спецификация и контроль действий пользователей над информационными ресурсами организации не осуществляется в полной мере и не отвечает требованиям безопасности.

Программно-аппаратные средства защиты информации:

1. Для защиты от несанкционированного проникновения и утечки информации предлагается использование межсетевых экранов или брандмауэров. Фактически брандмауэр — это шлюз, который выполняет функции защиты сети от несанкционированного доступа из вне (например, из другой сети).

Различают три типа брандмауэров:

1. Шлюз уровня приложений. Шлюз уровня приложений часто называют прокси-сервером (proxy-server) — выполняет функции ретранслятора данных для ограниченного числа приложений пользователя. То есть, если в шлюзе не организована поддержка того или иного приложения, то соответствующий сервис не предоставляется, и данные соответствующего типа не могут пройти через брандмауэр.

2. Фильтрирующий маршрутизатор. Маршрутизатор или программа на сервере, в дополнительные функции которого входит фильтрование пакетов (packet-filtering router). Конфигурация настраивается таким образом, чтобы фильтровать входящие и исходящие пакеты на основе анализа их адресов и портов. Брандмауэры такого типа обычно реализуются в виде списка правил, применяемых к значениям полей заголовка транспортного уровня.

3. Шлюз уровня коммутации. Защита реализуется в плоскости управления путем разрешения или запрета тех или иных соединений.

В ООО «Global Truck Sales» для устранения вирусов в системе используются антивирусная система Dr.Web Anti-Virus.

Dr. Web — антивирусы этого семейства предназначены для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, макровирусов, вирусов, поражающих документы MS Office, скрипт-вирусов, шпионского ПО (spyware), программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО (adware), потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов, а также от спама, скаминг-, фарминг-, фишинг-сообщений и технического спама, проверку памяти, использование нескольких ресурсов, защиту резидентов, обнаружение троянских программ.

Характерной особенностью антивируса Dr. Web является возможность установки на зараженную машину. В процессе установки производится сканирование памяти и файлов автозагрузки, перед сканированием производит-

ся обновление вирусной базы. При этом онлайн-обновления производятся каждый час, пользовательский интерфейс простой и интуитивно понятный.

Встроенный Windows Backup для создания архивов.

OS Backup Wizard — программа, предназначенная для быстрого создания и восстановления резервной копии Windows. Она позволяет создать копию всей Windows или только отдельных файлов и папок.

1.2.8 Недостатки в системе защиты информации

Специфика данного аспекта безопасности состоит в том, что информационная безопасность есть составная часть информационных технологий — области, которая развивается невероятно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, но и механизмы создания новых решений, позволяющие не отставать от технического прогресса.

Современные технологии программирования не позволяют создавать программы, работающие безошибочно, что не способствует быстрому развитию средств обеспечения информационной безопасности.

Говоря о текущем состоянии проблемы обеспечения информационной безопасности в исследуемой компании, наибольшую угрозу данным, их сохранности и конфиденциальности несет отсутствие регламентированной политики информационной безопасности, отсутствует как таковая защита данных внутри компании, документы и персональные данные передаются путем Skype и электронной почты, находящейся на сторонних серверах. Исходя из этого, задачей данной работы будет являться разработка сборника инструкций по политики безопасности компании ООО «Global Truck Sales», регламентация разграничения уровней доступа пользователей, внедрение политики информационной безопасности для использования в компании ООО

«Global Truck Sales», а также составление списка рекомендаций по обеспечению информационной безопасности для руководителя организации.

В ООО «Global Truck Sales» безопасности информации уделяется слишком мало внимания, хотя информация, которую может получить злоумышленник имеет немалую стоимость, независимо от того, какие цели преследует злоумышленник, будь то зачистка данных, их кража или передача конкурентам. Например, доступ к ПК может получить любой сотрудник или простой посетитель офиса из-за отсутствия как таковой системы контроля учета доступа в офисную часть, а также отсутствия учетной записи пользователей Windows, пароль на ПК каждый сотрудник устанавливает самостоятельно, что может усложнить доступ к ПК, например, при конфликтном увольнении сотрудника. Все вышеперечисленное является очень важными недостатками обеспечения информационной безопасности предприятия.

1.2.9 Мероприятия и средства по совершенствованию системы информационной безопасности

Для выполнения поставленных целей и решению задач необходимо провести мероприятия на уровнях информационной безопасности.

Административный уровень информационной безопасности.

Политика безопасности — это совокупность законов, правил и норм поведения, направленных на защиту информации и ассоциированных с ней ресурсов.

Следует отметить, что разрабатываемая политика должна согласовываться с существующими законами и правилами, относящимися к организа-

ции, т.е. эти законы и правила необходимо выявлять и принимать во внимание при разработке политики.

Чем надежнее система, тем строже и многообразнее должна быть политика безопасности.

В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы [3].

Организационный уровень защиты информации.

Важно место в системе организационных, административных, правовых и других мер, позволяющих качественно решать задачи информационного обеспечения научно-производственной и коммерческой деятельности, физической сохранности материальных носителей закрытых сведений, предотвращения их утечки, сохранения коммерческой тайны занимает разрешительная система доступа исполнителей к классифицированным документам и сведениям.

С учетом Федерального закона от 29.07.2004 № 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне»: «Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона» [17].

При составлении системы мер безопасности существенное внимание необходимо уделить оптимальному распределению производственных, коммерческих, финансовых сведений, оставляющих тайну предприятия, между конкретными исполнителями соответствующих работ и документов. При распределении информации, необходимо обеспечить предоставление конкретному сотруднику для качественного и своевременного выполнения порученных ему работ полного объема данных, а также, исключить ознакомление исполнителя с излишними, не нужными ему для работы классифицированными сведениями.

Для обеспечения правомерного и обоснованного доступа сотрудников к сведениям, составляющим коммерческую тайну компании, необходимо

разработать и внедрить на предприятии соответствующую разрешительную систему доступа к информации.

Под доступом понимается получение письменного разрешения руководителя организации (или, других уполномоченных лиц) на выдачу тому или иному сотруднику конкретных (или в полном объеме) закрытых сведений с учетом его должностных полномочий.

Разрешительная система должна:

- распространяться на все виды классифицированных документов, имеющихся на предприятии, независимо от их местонахождения и создания;
- определять порядок доступа всех категорий сотрудников, получивших право работать с информацией, а также специалистов, временно прибывших на предприятие и имеющих доступ к закрытым ресурсам;
- устанавливать простой и надежный порядок оформления разрешений на доступ к охраняемым документам;
- четко разграничивать права руководителей различных должностных уровней в оформлении доступа соответствующих категорий исполнителей;
- исключать возможность бесконтрольной и несанкционированной выдачи документов;
- запрещать лицам, работающим с классифицированной информацией и объектами, вносить изменения в учетные данные, а также подменять учетные документы.

Программно-технические меры защиты информации:

1. Регулярно читать специальную и периодическую литературу по проблеме безопасности и ЗИ, а полученные сведения об угрозах, средствах защиты, т.п. транслировать на свои объекты защиты.

2. Совершенствовать СЗ и СЗИ согласно новейшим достижениям науки и техники.

3. При создании или проверке существующих СЗ их необходимо рассматривать с точки зрения предложенных принципов, так как при детальном

анализе СЗ можно проявить нештатные ситуации, которыми может воспользоваться злоумышленник.

4. Изложенные принципы применимы для создания разных концепций защиты объектов, начиная от пожарно-охранной безопасности и заканчивая СЗИ.

5. При проектировании или усовершенствовании существующих СЗ для их объективной оценки следует привлекать сторонние организации, которые имеют лицензии на соответствующие виды деятельности.

6. Данные принципы оказывают существенную помощь в процессе контроля защищенности объектов при условии их детализации применительно к конкретным условиям.

7. Проводить регулярный и комплексный контроль всех мероприятий по обеспечению безопасности и ЗИ.

8. Подготовить и воплотить в жизнь мероприятия по «защите персонала».

9. Составить подробный перечень возможных угроз для каждой технологии работы с объектами защиты.

10. Определить перечень внештатных ситуаций и меры по их ликвидации.

11. Готовить персонал к регламентированным действиям во внештатных ситуациях.

12. Проводить регистрацию и анализ текущей деятельности с целью определения возможных угроз и внештатных ситуаций.

13. Проводить разъяснительную работу и учебу с персоналом, используя разные средства (тренинг, инструктаж, наглядная агитация, профилактические проверки и т.д.).

14. Планировать и вести обучение, а также специальные проверки персонала по всем вопросам безопасности и ЗИ.

15. Проведение работ по обеспечению безопасности необходимо выполнять согласно действующей в стране нормативно-правовой системе.

Вывод: Современная система информационной безопасности представляет из себя синтез организационных и программно-технических мер, реализованных на основе единого подхода. При этом организационные меры не менее важны, чем технические — без внедрения безопасных приемов работы и осознания необходимости принимаемых мер, немыслимо создать действительно защищенную инфраструктуру безопасности.

Разработка политики информационной безопасности для компании ООО «Global Truck Sales» будет состоять из следующих этапов:

- анализ и аудит информационных и технических активов предприятия;
- определение уровня безопасности для каждого актива;
- определение средств обеспечения безопасности и их рентабельности;
- создание политики безопасности компании ООО «Global Truck Sales»;
- создание нормативных актов соблюдения политики безопасности в ООО «Global Truck Sales».

Результатом данной работы будет являться электронный сборник инструкций, представляющий собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности, практических работ для IT-специалистов и заданий в тестовой форме для сотрудников.

На сегодняшний день составлен план мероприятий по совершенствованию информационной защиты и выглядит следующим образом:

Разовые мероприятия:

1. Ознакомление сотрудников со сборником электронных инструкций по информационной безопасности (ответственные – руководители отделов).

2. Проверка знания инструкций по информационной безопасности (ответственные – руководители отделов).

3. Определение прав доступа для разных уровней должностей, разграничение доступа посредством Active Directory (ответственные — руководители отделов, исполнители — IT-специалисты).

4. Установка источника бесперебойного питания, для автономной работы офиса (ответственный — директор филиала).

5. Составление чек-листа периодических проверок сотрудников IT-специалистом, на предмет соблюдения правил информационной безопасности (ответственные — IT-специалисты, служба безопасности).

6. Проведение с привлечением экспертов анализа состояния защиты и оценки эффективности применяемых защитных мер, принятие на основе экспертного заключения необходимых мер по совершенствованию системы защиты (ответственный — директор филиала).

7. Опись материальных ценностей компании.

8. Подписание договоров материальной ответственности всеми сотрудниками, использующими портативную корпоративную технику, такую как: ноутбуки, смартфоны (ответственные — директор филиала).

9. Внедрение должности тренинг-менеджера (совмещение), обучение сотрудника, по итогу обучения — выдача сертификата на 16 часов обучения.

10. Блокирование USB-портов от подключения внешних носителей на клиентских ПК (ответственные — IT-специалисты). Доступ к USB-портам сохраняется у директоров филиалов и IT-специалистов.

11. Обеспечить наличие резервного клиентского ПК (ответственные — IT-специалисты, директор филиала).

12. Настройка принудительной блокировки ПК через 2 минуты бездействия (ответственные — IT-специалисты)

Срок завершения разовых мероприятий: 31.03.2019

Периодически проводимые мероприятия:

1. Ведение учета материальных ценностей компании посредством проведения инвентаризации оборудования (один раз в 6 месяцев, ответственный — IT-специалист, директор филиала).

2. Ведение и анализ системных журналов, принятие мер по обнаруженным нарушениям (ответственные — IT-специалисты, директор филиала).

3. Проведение обучающих тренингов по защите информации на регулярной основе затрагивающих такие темы, как: антивирусная защита, парольная защита сотрудников (ответственные — тренинг-менеджер, IT-специалисты).

Мероприятия, проводимые по необходимости:

1. Тестирование обновлений на специализированных компьютерах для выявления возможных проблем (ответственные — IT-специалисты, директор филиала).

2. Обучение правилам информационной безопасности на предприятии новых сотрудников (ответственные — тренинг-менеджер, IT-специалисты).

3. Обучение действующих сотрудников новым инструкциям и регламентам сотрудников (ответственные — тренинг-менеджер, IT-специалисты).

1.3 Основы разработки сборника электронный инструкций

1.3.1 Теоретические основы разработки набора электронный инструкций

Набор электронных инструкций, очень часто встречающаяся форма подачи нового материала. Кроме того, электронные ресурсы такого рода могут содержать одновременно практические работы, тренажеры, а также различные тесты, т.е. одновременно это является и программным обеспечением по подаче знаний и по их контролю.

Электронные инструкции имеют совокупность параграфов определенных видов. Эти типы — алгоритмы, доказательства, примеры, пояснения, теоремы, определения и др. В данном проекте изученная система работает с главными типами параграфов — с теоремами и определениями.

Электронный сборник должен предоставлять аналогичные (близкие к реальности) возможности. В нем, например, можно использовать на порядок больше иллюстраций, чем в обычном учебнике, фрагменты видеофильмов, а можно использовать панорамы виртуальной реальности, с помощью которых на экране компьютера можно получить полное представление об окружающей обстановке, в том числе и об источниках звука, рассмотреть подробнее определенные предметы и даже прочитать их описание или прослушать (продолжая их рассматривание) эту же информацию [24].

Применение электронного сборника в учебном процессе может повлиять на:

- повышение целенаправленности;
- усиление мотивации;
- повышение информативной емкости учебного содержания;
- активизацию учебно-познавательной деятельности обучаемых;
- ускорение темпа учебных действий.

1.3.2 Система дистанционного обучения и электронные инструкции

Дистанционное обучение содержит технологии, реализуемые, в основном, с использованием информационных и телекоммуникационных технологий при опосредованном (на расстоянии) или не полностью опосредованном содействии обучающегося и преподавателя.

Целью применения дистанционного обучения считается предоставление обучающимся возможности освоения образовательных программ, а именно по месту жительства (или временного пребывания) в комфортное для него время и в комфортном для него темпе.

Для обучения с использованием дистанционных технологий ученик должен иметь возможность доступа в Интернет и владеть комплектом компьютерных программ в пределах офисного пакета, программ для чтения гра-

фического текстового формата .pdf, а, так же, для просмотра графических файлов.

Как правило, в дистанционном обучении используются электронные учебники. Преимуществами этих учебников считаются: их мобильность; доступность связи с развитием компьютерных сетей; адекватность уровню развития современных научных знаний.

С другой стороны, создание электронных сборников способствует также решению и такой проблемы, как систематическое обновление информационного материала. В них также может содержаться большое количество упражнений и примеров, подробно иллюстрироваться в динамике различные виды информации.

1.3.3 Применение набора электронных инструкций в образовательном процессе

Практика применения сборников электронных инструкций в образовательном процессе показала, что учащиеся качественно усваивают изложенный материал, о чем свидетельствуют результаты научных тестирований.

Таким образом, развитие информационных технологий дает широкую возможность для изобретения новых методик в образовании и тем самым увеличивается качество образования.

Электронный сборник инструкций часто дополняет обычный учебник, тем самым повышается эффективность в тех случаях, когда он: гарантирует буквально моментальную обратную связь; помогает быстро найти нужную информацию (в том числе контекстный поиск), поиск которой в обычном учебнике затруднен; существенно экономит время при неоднократных обращениях к гипертекстовым объяснениям; наряду с кратким текстом — демонстрирует, рассказывает, моделирует и т.д. (именно здесь проявляются возможности и преимущества мультимедиа технологий) позволяет быстро, но в

темпе более оптимальном для определенного индивида, проверить знания по конкретному разделу.

К недостаткам электронных ресурсов такого рода можно отнести особенности работы с дисплеями рабочей станции (восприятие с экрана текстовой информации гораздо менее удобно и эффективно, чем чтение книги).

1.3.4 Определение понятия электронного сборника инструкций среди других аналогичных

Электронный сборник инструкций — это компьютерная программа, которая имеет набор средств для простого поиска и навигации по своему содержимому [23].

Электронным сборником инструкций является продукт образовательного характера, способный быть воспроизведенным или использованным только с помощью предметов информатики, например компьютера, соответствующий утвержденному содержанию обучения или программе, которая разработана автором для предложенной специальности и предмета.

Электронный сборник становится инструментом познания и обучения, его содержание и структура зависят от целей и задач его использования. Он может выполнять функции репетитора, самоучителя и тренажера. Особую значимость он имеет при использовании в системах телекоммуникации.

1.3.5 Общие требования к представлению информации в электронном виде

Применение электронного сборника инструкций должно быть эффективным за счет выполнения следующих требований:

1. Учебный материал должен предоставляться с необходимой степенью наглядности, за счет возможности его динамического отображения

(например, flash-анимация, видеоролики и др.), также оформляться учебный материал должен для различных категорий пользователей.

2. Электронные средства обучения должны характеризоваться компактностью и мобильностью.

3. Должен иметься процесс поиска необходимой информации достаточно удобно и очень быстро.

4. Необходимо наличие электронных средств проверки знаний, которые позволят проводить объективный контроль и оценку уровня знаний и навыков. Средствами контроля оценки уровня знаний могут являться такие инструменты, как: задания в тестовой форме, интерактивные средства проверки знаний.

Для того, чтобы электронный сборник инструкций мог выполнять в полном объеме возложенные на него учебные задачи необходимо, чтобы он соответствовал следующим характеристикам:

1. Целостность. Под целостностью понимается всестороннее представление на основе принципа учета междисциплинарных связей содержания изучаемого предмета.

2. Научность. Данная характеристика подразумевает использование терминологии, которая соответствует современным научным требованиям изучаемой области предметных знаний, а также однозначную трактовку терминов и достоверность предоставляемых научных знаний.

3. Системность. Под системностью подразумевается разбиение учебного материала на разделы и подразделы (модули и микромодули), последовательность изложения материала и требование логической взаимосвязанности разделов (модулей).

4. Функциональность. Под функциональностью подразумевается возможность виртуального выполнения определенных функций, направленных на приобретение конкретных умений по дисциплине.

5. Наглядность. Эффективные иллюстрации, которые позволяют осознать, осмыслить и запомнить учебный материал, обеспечивают наглядность. Данную характеристику также следует рассматривать через эргономику.

6. Интерактивность. Интерактивность характеризуется не только наличием эффективной обратной связи, но и возможностью общения пользователя в процессе работы с системой» [22].

1.3.6 Принципы создания электронного сборника инструкций

Современные электронные обучающие ресурсы должны обеспечивать творческую деятельность обучающегося с моделями систем взаимодействующих объектов и с объектами изучения. Именно творческая деятельность, лучше в рамках работы, сформулированной преподавателем, способствует закреплению и формированию комплекса умений и навыков у учащегося. Креативная область позволяет организовать коллективную деятельность учащихся над проектом.

Принцип авторской среды. Электронный сборник должен подходить и быть адаптируем к учебной деятельности. То есть позволять учесть особенности конкретного ученика, конкретной специальности, конкретного предмета обучения. Для этого необходима подходящая авторская среда. Она будет обеспечивать включение дополнительной информации в электронную энциклопедию, поможет пополнять задачник, готовить предоставляемые материалы и учебные пособия по предмету. По факту, это подобие инструмента, используя который создается сам сборник электронных инструкций.

Невербальная среда. Стандартно электронные ресурсы вербальны в своей сути. Они излагают теорию в графической или текстовой форме. Это является продолжением полиграфических изданий. Но в сборнике электронных инструкций возможно реализовать метод «делай как я». Данная среда наделяет сборник электронных инструкций чертами живого учителя. Данные формы представления материала бывают реализованы в виде определенных

электронных учебников или сгруппированы в рамках одного ансамбля. Все зависит от основы «автора». Автор должен иметь знания об истории и всех возможностях электронных ресурсов такого рода. Хорошим сборник электронных инструкций будет в том случае, когда он «впишется» в процесс обучения.

1.3.7 Практические задачи в электронном сборнике

Одной из важных составляющих электронного сборника инструкций являются практические задания. Практические задания содержат упражнения, позволяющие практическую отработку умений, с внедрением в них теоретической информации, что позволяет обучаемому наилучшим образом усвоить материал, а обучающему не нужно подбирать слова для каждого ученика, достаточно показать практически.

В практикуме могут имеется пошаговые решения типичных упражнений и задач по определенному учебному курсу с разнообразными пояснениями. В качестве стандартных заданий можно отметить наглядные компьютерные модели. Создание электронных практических заданий содержит 8 этапов:

1. Подбор литературы, как электронной, так и печатной, которые удобны для составления гипертекстов и содержат большое количество задач и примеров.

2. Разбивка материала на части, состоящие из модулей, и еще составление глоссария, которые нужны для овладения предметом.

3. Изменение и редактирование текстов источников по структуре, имеющей оглавление, содержание модулей.

4. Добавление и исключение необходимых материалов и текстов, определение связей между структурой и другие взаимосвязанные гипертекстные.

5. Реализация в электронной форме гипертекста.

В результате собирается электронный сборник, который готов к использованию в целях учебы.

Для реализации наполнения сборника необходимо следовать следующим пунктам:

6. Выбор глав пособия, в которых необходимо текст заменить наглядными мультимедийными примерами, при необходимости делается или подбирается озвучка.

7. Разработка содержания визуализации модулей для получения наибольшей наглядности, максимального освобождения экрана от текстовых вставок и использования эмоциональной памяти учеников для облегчения запоминания и понимания изучаемого материала.

8. Визуализация текстов, то есть компьютерное воплощение разработанного содержания с использованием рисунков, анимации и графиков.

Визуализации стоит уделить особое внимание, так как наглядность — один из наиболее удобных и доступных методов обучения, который позволяет наилучшим образом усвоить подаваемый материал обучаемому.

2 ХАРАКТЕРИСТИКА ЭЛЕКТРОННОГО СБОРНИКА ИНСТРУКЦИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОТРУДНИКОВ ПРЕДПРИЯТИЯ «GLOBAL TRUCK SALES»

2.1 Точный и расширенный педагогические адреса

Точный педагогический адрес: набор электронных инструкций разработан для поступивших на работу сотрудников ООО «Global Truck Sales».

Расширенный педагогический адрес: набор электронных инструкций может быть использовано всеми сотрудниками ООО «Global Truck Sales», для актуализации знаний.

2.2 Структура сборника электронных инструкций

Сборник электронных инструкций можно разделить на 3 блока:

- методический блок;
- обучающий блок;
- блок контроля.

Методический блок представлен инструкцией к изучению ресурса на главной странице. Обучающий блок представлен инструкциями, согласованными службой безопасности и дирекцией ООО «Global Truck Sales» и практическими работами для IT-специалистов. Блок контроля включает в себя задания в тестовой форме.

2.3 Навигация

Навигация по электронному сборнику представлена наличием основного меню на верхней панели с разделами: главная, инструкции, IT-специалистам. Блоки основного меню представлены на рисунке 4.

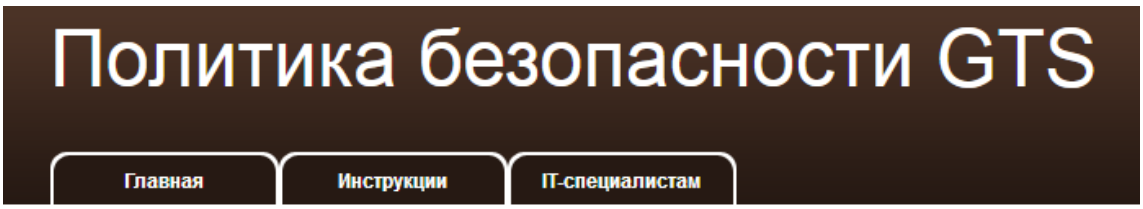


Рисунок 4 — Блоки основного меню

Набор инструкций доступен по кнопке «Инструкции» основного меню, навигация осуществляется посредством гиперссылок на страницы сайта (рисунок 5).

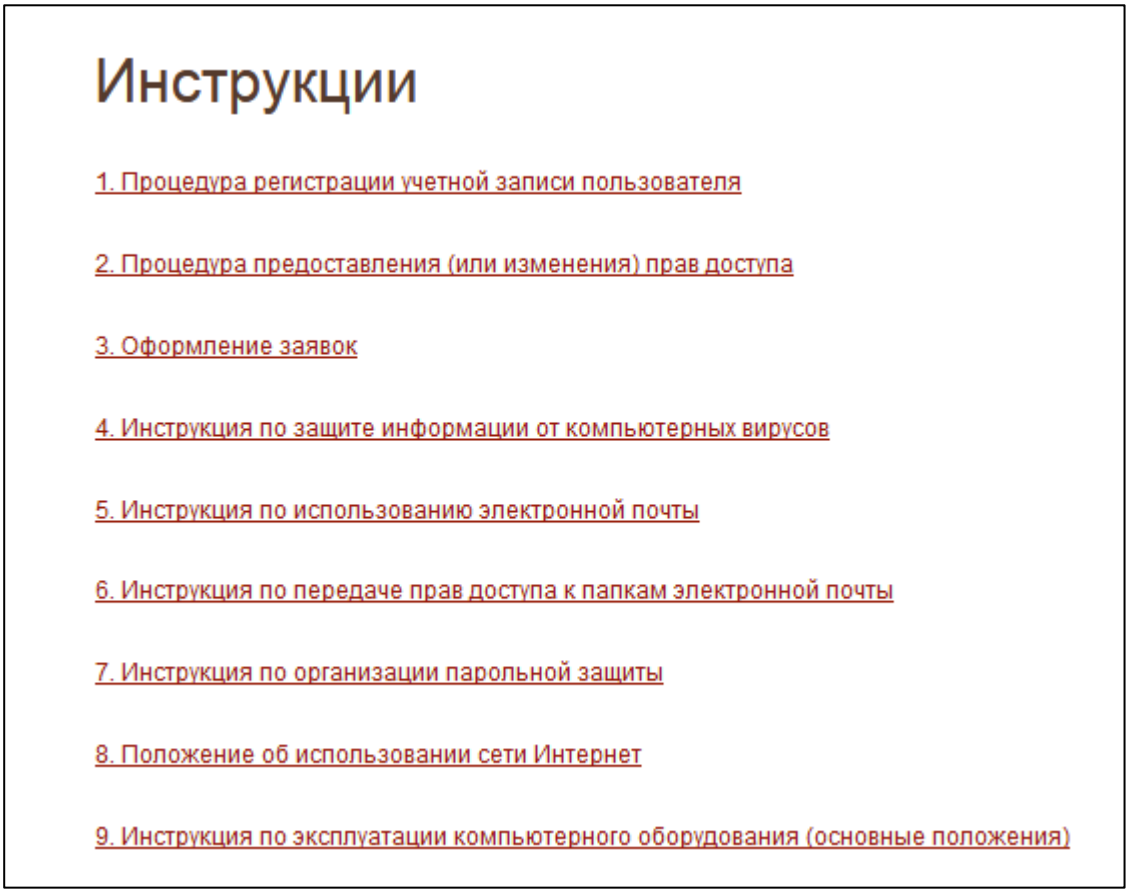


Рисунок 5 — Список инструкций

Инструкции обязательны для ознакомления всем сотрудникам, имеющим или получающим доступ к АРМ.

Практических блоки для IT-специалистов (рисунок 6), представляют собой пошаговые инструкции для добавления пользователя в Active Directory, управление групповыми политиками Active Directory и разрешение на удаленное подключение.

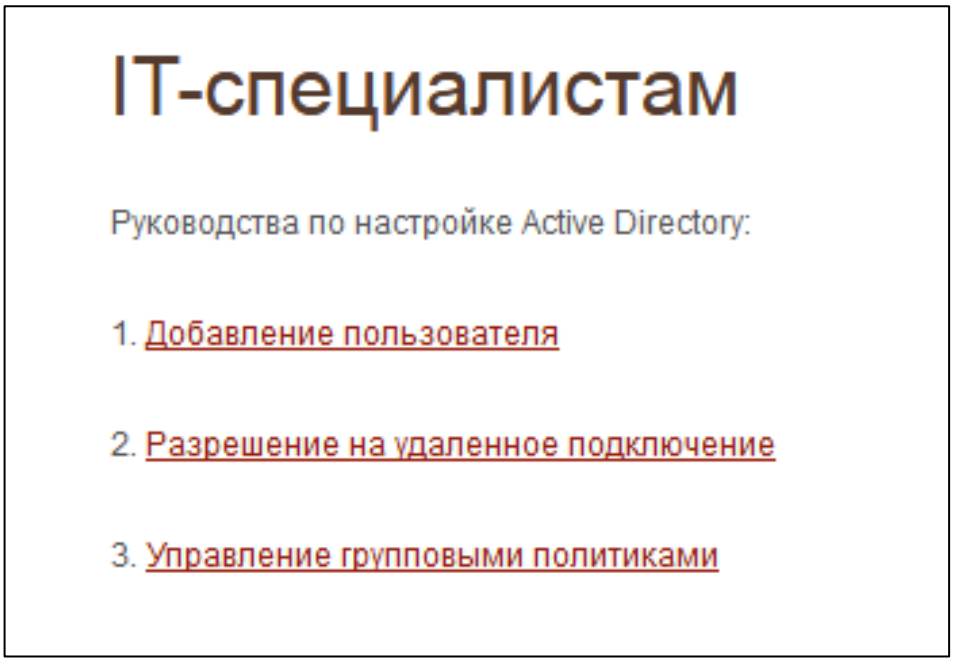


Рисунок 6 — Блок IT-специалистам

Блок проверки (рисунок 7) включает в себя гиперссылки на задания в тестовой форме. По итогу прохождения заданий в тестовой форме пользователи получают разрешение на использование ПК.

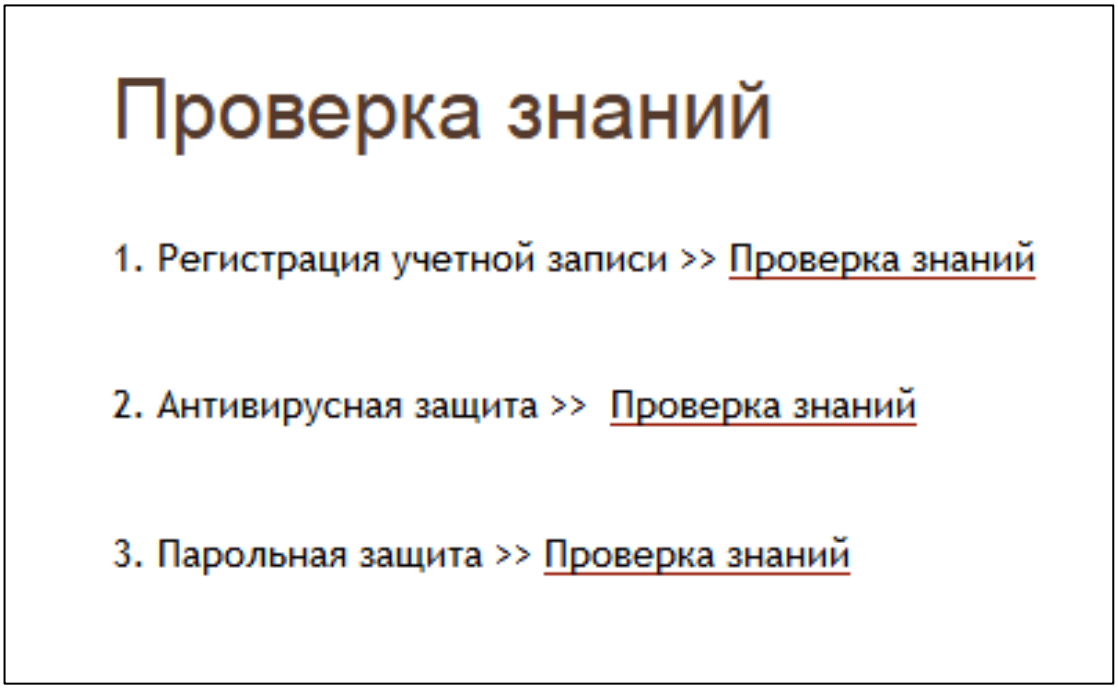


Рисунок 7 — Блок проверки знаний

2.4 Интерфейс

Сборник электронных инструкций состоит из логически связанных html-страниц, упорядоченных по смыслу. В электронном сборнике управление осуществляется через пункты основного меню, а также через гиперссылки.

Практические задания для IT-специалистов по обучению работе в Active Directory, в разработанном сборнике инструкций включает в себя разделы:

- практика;
- теория.

Начальная страница набора электронных инструкций (index.html) приведена на рисунке 8.

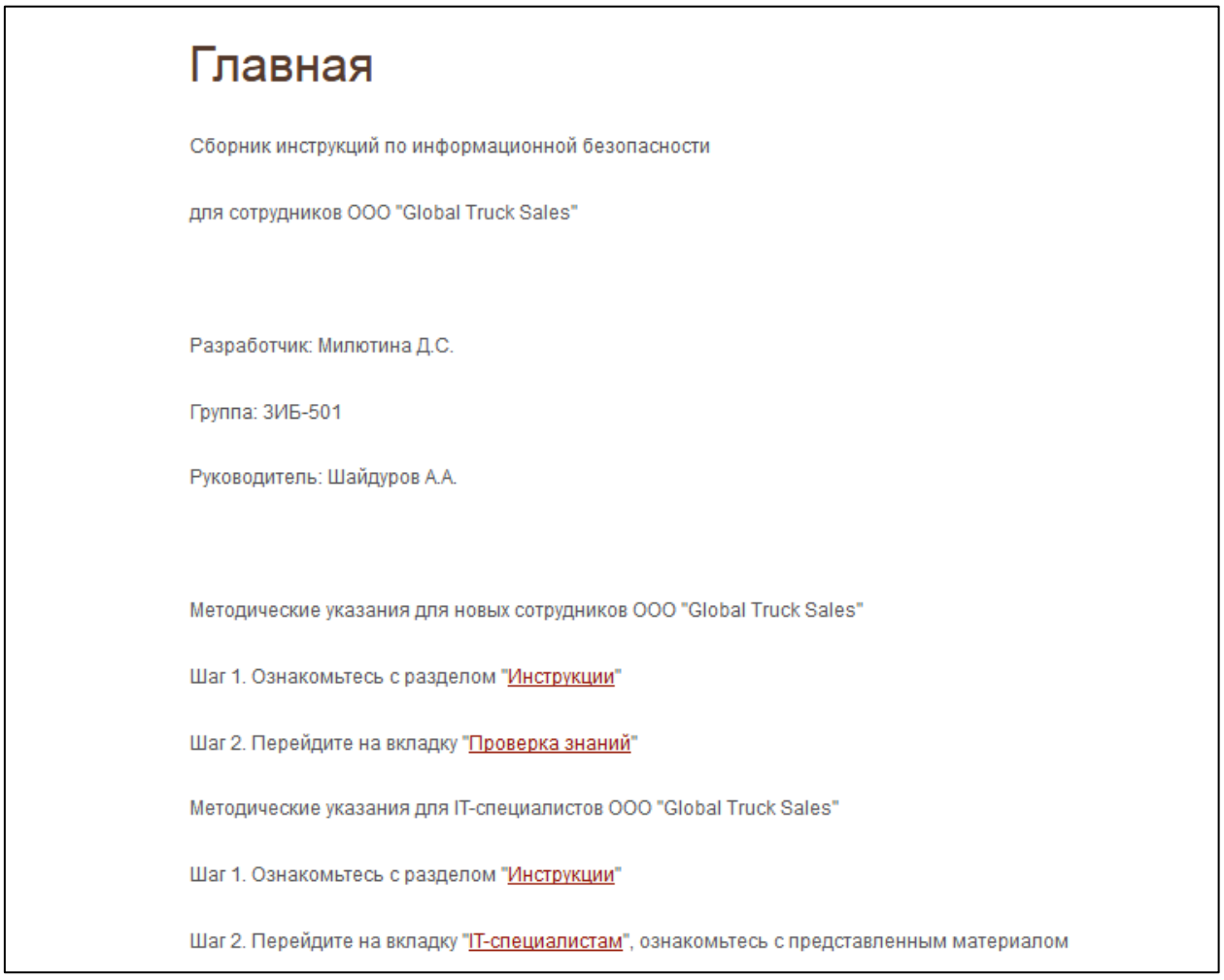
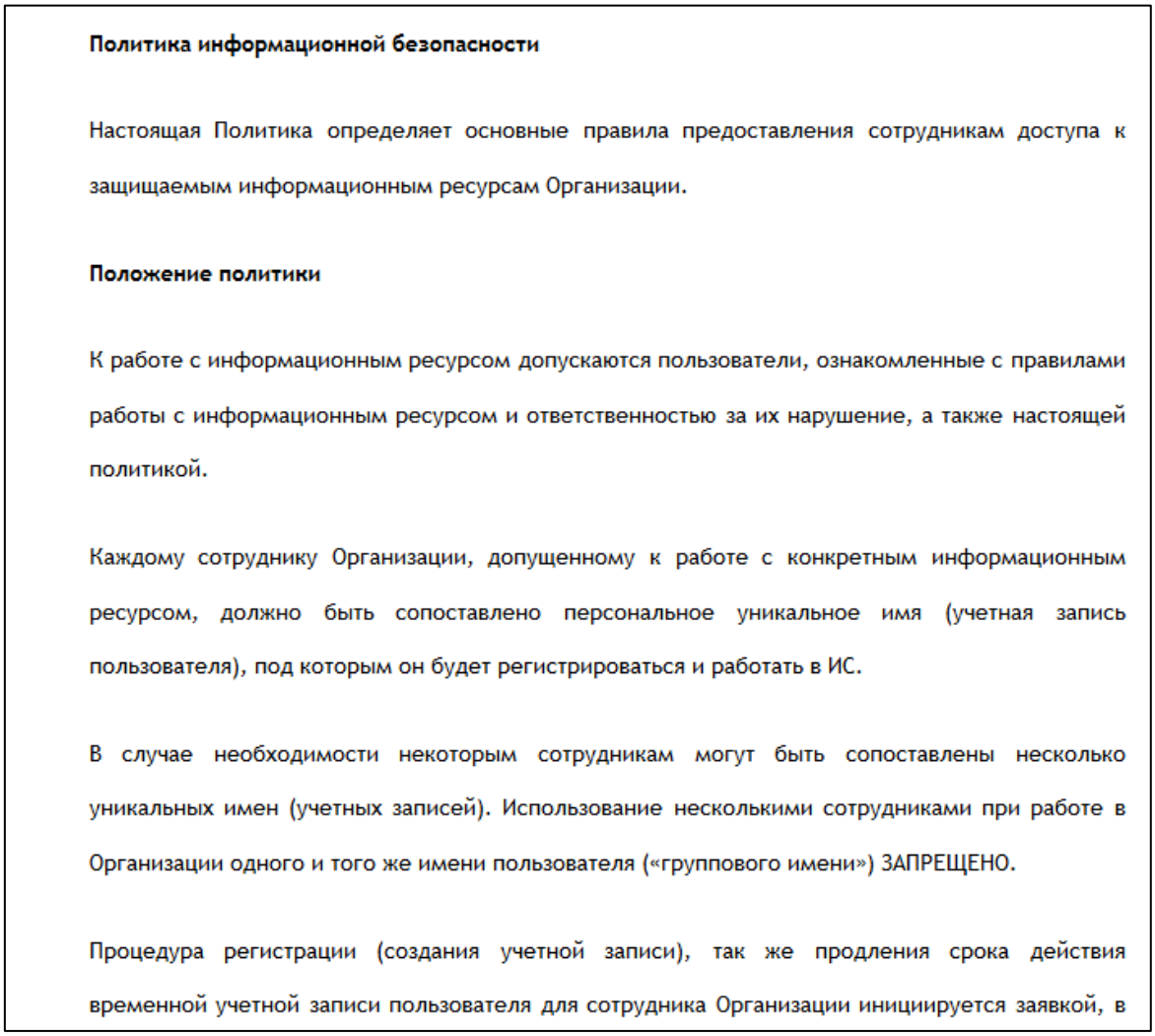


Рисунок 8 — Стартовая страница набора электронных инструкций

Теоретический материал представлен в виде инструкций для сотрудников, обязателен к изучению всем сотрудникам компании и является обязательным к изучению для всех новых сотрудников. По итогу изучения теоретического материала сотруднику необходимо выполнить задания в тестовой форме. Доля правильных ответов должна быть не менее 80%.

Содержание теоретического материала:

Тема 1. Выдержка из Политики информационной безопасности: Процедура регистрации пользователей (рисунок 9).



Политика информационной безопасности

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам Организации.

Положение политики

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику Организации, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

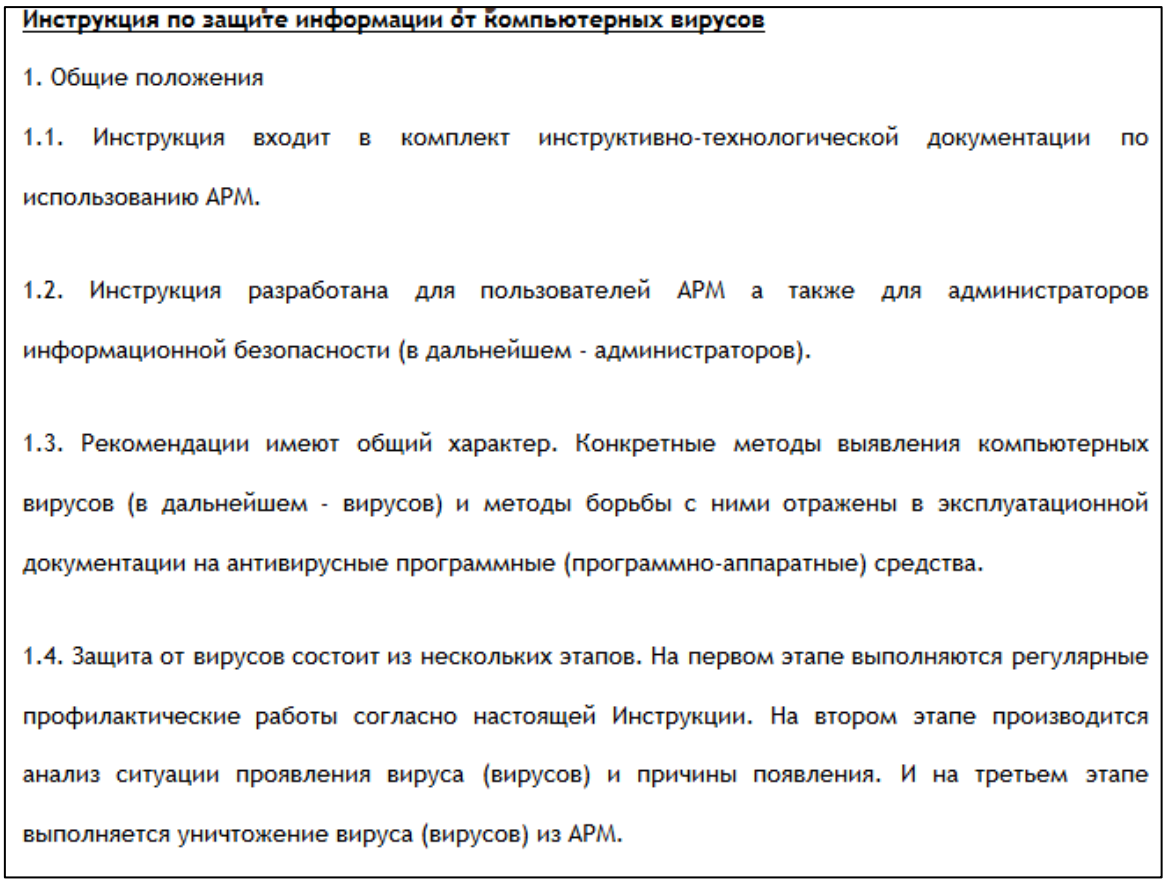
В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Организации одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Организации инициируется заявкой, в

Рисунок 9 — Пример страницы инструкции доступа к информационным ресурсам

Понятия: информации, «информационный ресурс». Персональное уникальное имя, процедура регистрации, порядок формирования заявки на получение, удаление, изменение учетной записи и/или прав доступа к информационному ресурсу.

Тема 2. Инструкция по защите информации от компьютерных вирусов (рисунок 10).



Инструкция по защите информации от компьютерных вирусов

1. Общие положения

1.1. Инструкция входит в комплект инструктивно-технологической документации по использованию АРМ.

1.2. Инструкция разработана для пользователей АРМ а также для администраторов информационной безопасности (в дальнейшем - администраторов).

1.3. Рекомендации имеют общий характер. Конкретные методы выявления компьютерных вирусов (в дальнейшем - вирусов) и методы борьбы с ними отражены в эксплуатационной документации на антивирусные программные (программно-аппаратные) средства.

1.4. Защита от вирусов состоит из нескольких этапов. На первом этапе выполняются регулярные профилактические работы согласно настоящей Инструкции. На втором этапе производится анализ ситуации проявления вируса (вирусов) и причины появления. И на третьем этапе выполняется уничтожение вируса (вирусов) из АРМ.

Рисунок 10 — Пример страницы по защите информации от компьютерных вирусов

Понятия: Этапы защиты от вирусов, методы борьбы с вирусами, наиболее характерные внешние проявления вирусов, виды вирусов, профилактика вирусов, регламент уничтожения вирусов.

Тема 3. Инструкция по использованию электронной почты.

Описывает регламент получения и использования электронного почтового адреса.

Тема 4. Инструкция по организации парольной защиты.

Включает в себя: Правила формирования личного пароля, правила ввода пароля, порядок смены паролей, порядок хранения паролей, ответственность при организации парольной защиты.

Тема 5. Положение об использовании сети Интернет.

Общие положения использования сети Интернет. Основные термины, сокращения и определения. Разграничение доступа к сети Интернет сотрудникам ООО «Global Truck Sales», правила использования сети Интернет.

Тема 6. Инструкция по эксплуатации компьютерного оборудования (основные положения).

Регламент и режимы работы компьютерного оборудования, порядок ввода в эксплуатацию и перемещение компьютерного оборудования, подготовка компьютерного оборудования к эксплуатации, эксплуатация компьютерного оборудования.

Раздел «Практика» содержит четыре практических работы, «Инструкция по передаче прав доступа к папкам электронной почты» необходима для изучения всем сотрудникам ООО «Global Truck Sales», руководства для настройки Active Directory (добавление пользователя, разрешение на удаленное подключение, управление групповыми политиками) необходимы для изучения IT-специалистам компании.

Каждая из работ представляет собой пошаговую инструкцию для выполнения поставленных задач. Знание сотрудниками инструкции по передаче прав доступа к папкам электронной почты позволяет минимизировать риск передачи паролей сотрудниками на период отпуска или больничного (рисунок 11).

В инструкциях для IT-специалистов представлено по 2 способа решения поставленных задач. Так как компания в данный момент находится на стадии развития и штат увеличивается, появляются новые должности и уровни должностей, IT-специалисты могут использовать эти инструкции практически на ежедневной основе. Кроме того, все инструкции адаптированы для предприятия и будут актуальны и для новых сотрудников в должности IT-специалистов.

Все инструкции размещены на внутреннем ресурсе, и при появлении новых инструкции и регламентов, учебный портал по информационной безопасности будет пополняться.

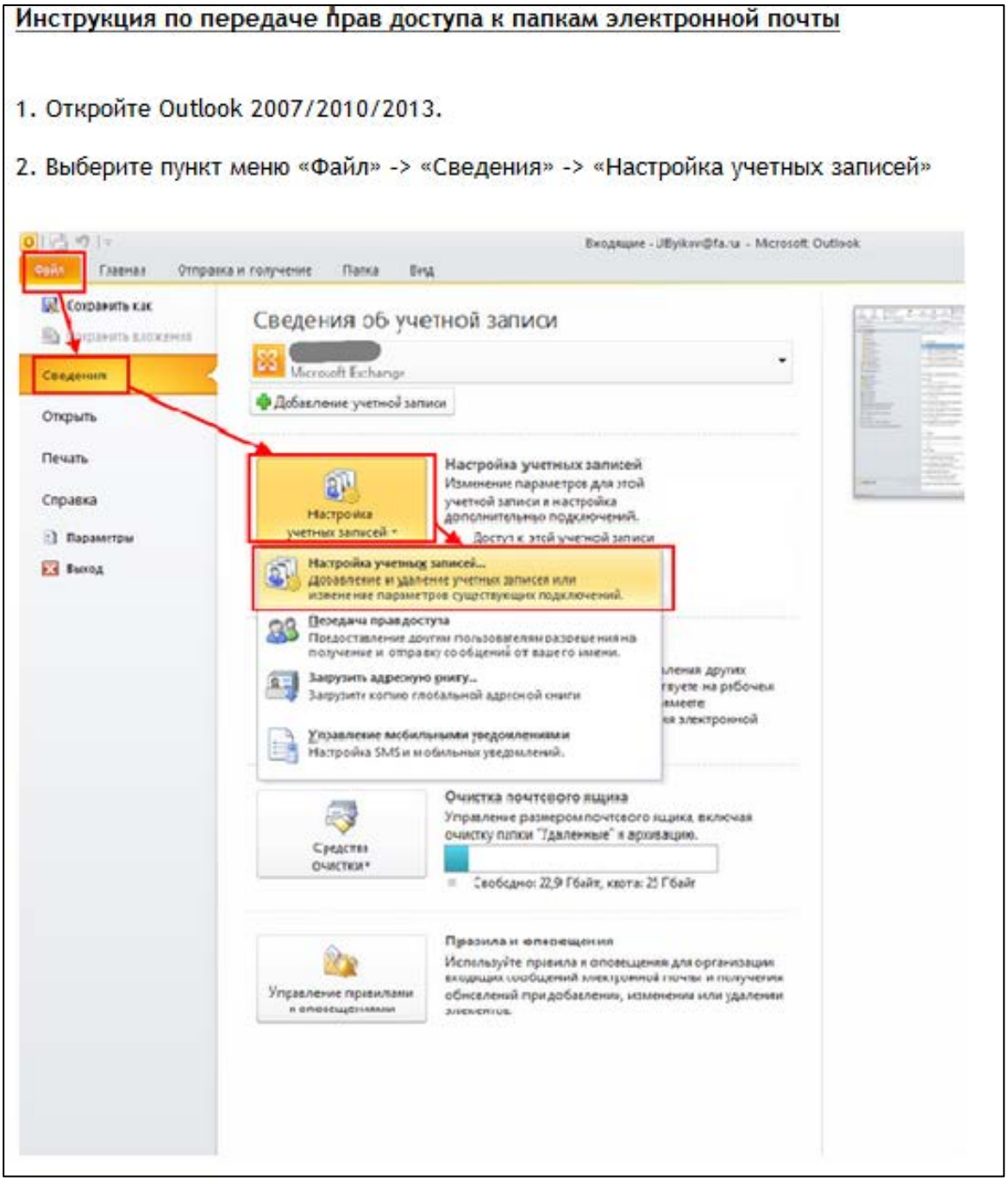


Рисунок 11 — Инструкция по передаче прав доступа к папкам электронной почты

Основные характеристики практической работы:

- самостоятельность деятельности сотрудников, обеспечивается при помощи методического выполнения заданий лабораторной работы;
- выполнение одной практической работы выполняется каждым сотрудником самостоятельно, при дальнейшей деятельности инструкции остаются доступны сотрудникам для избегания ошибок в работе.

Практические работы представлены в виде пошаговых инструкций, с наглядным пособием в виде картинок (рисунок 12, 13).

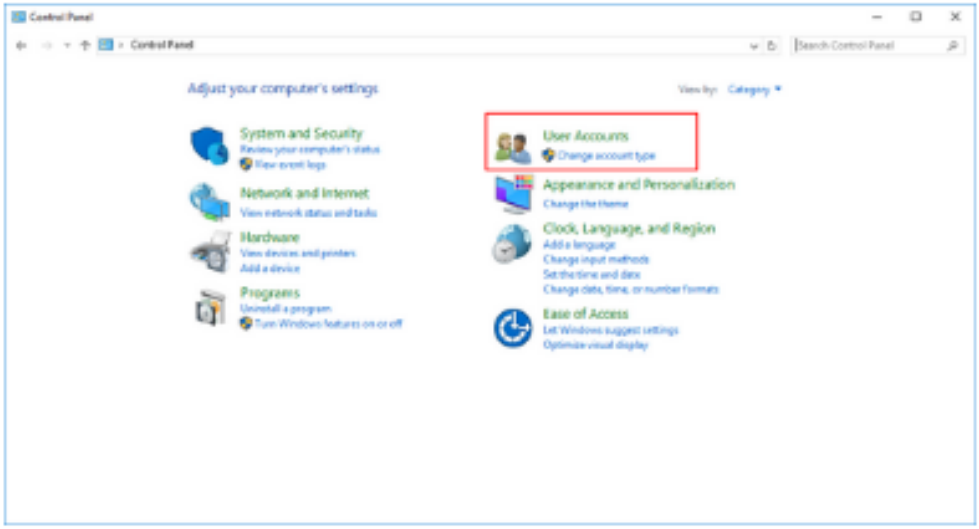
Добавление пользователя

Для того, чтобы еще один пользователь мог подключиться к виртуальному серверу с операционной системой Windows Server 2016, необходимо его создать и выдать права на удаленное подключение к серверу.

Создание пользователя

СПОСОБ 1

Для создания пользователя в Windows откройте Панель управления сервером и выберите вкладку User Accounts.



Далее снова перейдите во вкладку User Accounts.

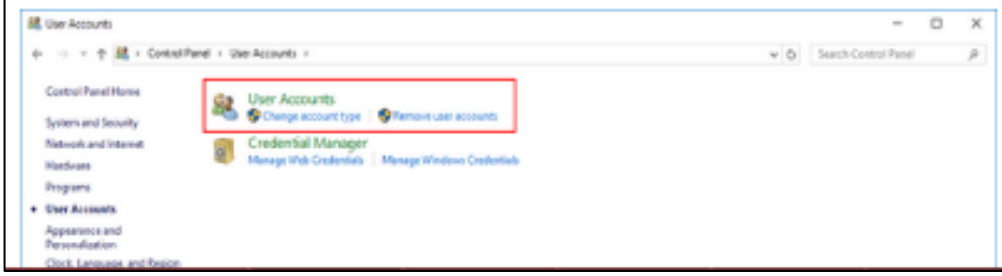


Рисунок 12 — Инструкция по добавлению пользователя Active Directory

Каждый шаг для выполнения задачи представлен на картинке и сопровождается текстовыми комментариями. Кроме того, необходимые действия выделены красным. Таким образом выполняется функция наглядности.

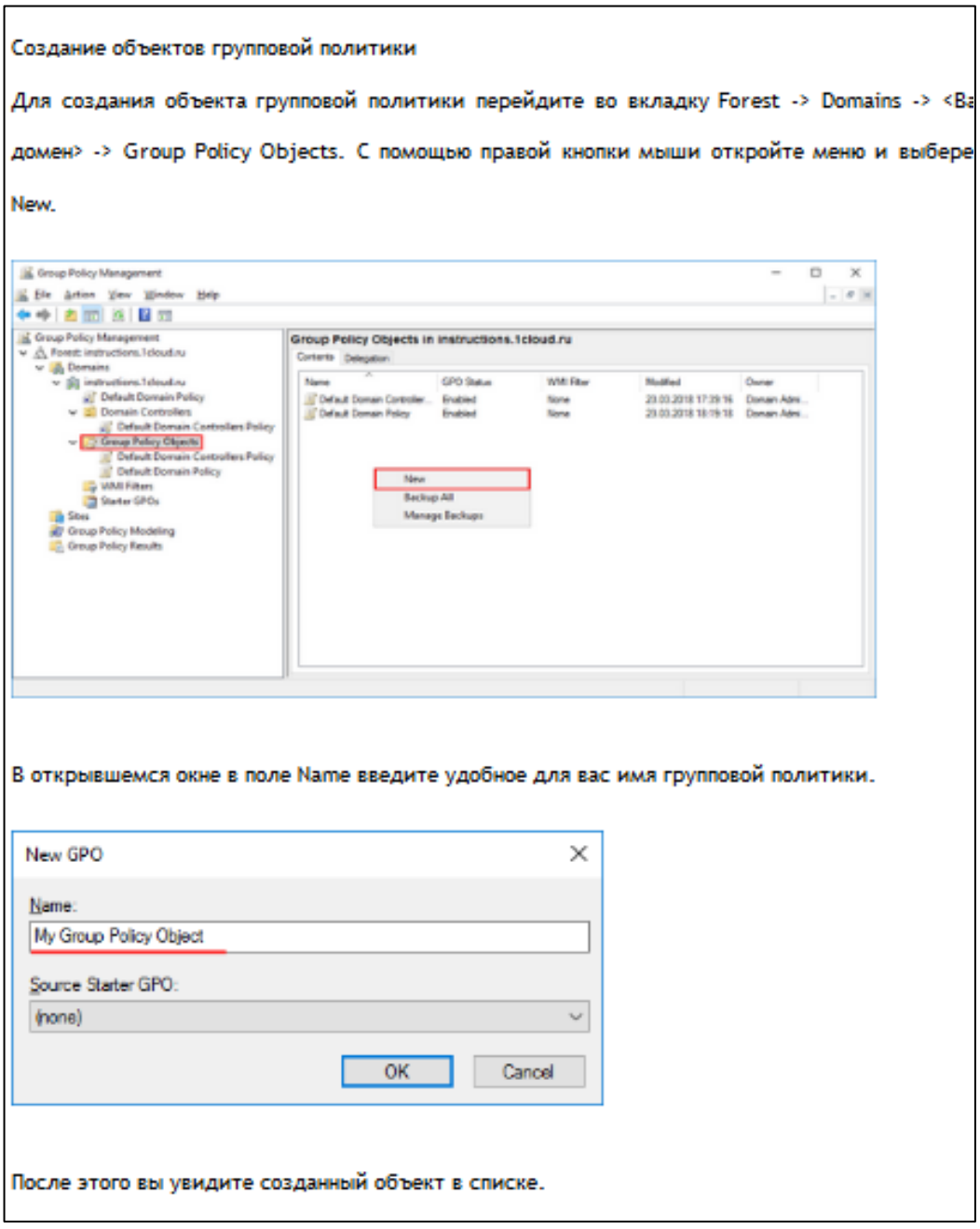


Рисунок 13 — Инструкция по управлению групповыми политиками Active Directory

2.5 Апробация практических заданий для IT-специалистов

Апробация проходила в период с 28.12.2018 г. по 29.12.2018 г. у действующих сотрудников отдела IT ООО «Global Truck Sales» в количестве

трех человек. После вводного инструктажа IT-специалисты приступили к выполнению практической работы №2 «Добавление пользователя». У сотрудников возникли проблемы с поиском необходимых ссылок. В связи с этим была добавлена ссылка IT-специалистам, для конкретизации доступа.

Выполнение практической работы №2 «Добавление пользователя» заняло от 20 до 30 минут. В связи с этим добавлен еще один способ выполнения данной практической работы. Практическую работу №2 руководитель службы безопасности принимал, проверив выполнение заданий и проверив знания устными вопросами.

Сотрудникам, сдавшим практическую работу №2, дали задание приступить к выполнению практической работы №3.

Вывод:

- добавлена ссылка «IT-специалистам»;
- добавлены дополнительные способы выполнения задач.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной работы было выяснено, что основной задачей политики информационной безопасности является минимизация рисков потери данных и утечки информации. Политика информационной безопасности представляет собой совокупность мер и регламентов по защите данных.

Однако, следует отметить, что снижение рисков для компании не должно сказываться на удобстве работы пользователей. Как показывает практика, большинство пользователей халатно относится к безопасности информации и хранению данных, из этого следует, что одна из главных задач политики информационной безопасности — регламентация условий хранения и передачи данных, для сохранения конфиденциальности, защиты от изменения информационных ресурсов.

Наиболее явно требования к документальному определению вопросов информационной безопасности указаны для предприятий, выпускающих оборонную продукцию — в ГОСТ 15.002-2000, где предусматривается обязательная программа обеспечения безопасности как часть политики качества. Указанный документ должен включать совокупность процедур, мероприятий и процессов обеспечения безопасности разработки (производства) СЗИ (составляющей гостайну), согласуется с представителем заказчика и подлежит обязательному инспекционному контролю.

Проведен анализ организации ООО «Global Truck Sales», в ходе анализа выявлена необходимость разработки Политики информационной безопасности компании, а также обучения сотрудников правилам соблюдения Политики информационной безопасности.

При написании дипломной работы была достигнута цель — разработано электронный сборник инструкций для обучения сотрудников ООО «Global Truck Sales».

Для достижения цели были решены следующие задачи:

- проанализирована общая характеристика объекта защиты в организации;
- проанализирована степень защищенности объектов защиты по каждому из видов защиты информации (ЗИ) (правовая ЗИ, организационная ЗИ, программно-аппаратная ЗИ, инженерно-физическая ЗИ);
- внесены такие предложения по защите информации, как: разграничение доступа к информационным ресурсам, установлен порядок смены и хранения паролей, регламентирована парольная защита, регламентирован порядок контроля доступа и проведено обновление существующих регламентов, установлен источник бесперебойного питания;
- разработано электронный сборник инструкций для обучения сотрудников основам информационной безопасности.

Таким образом, цель работы достигнута, поставленные задачи решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аграновский А. В. Основы технологии проектирования систем защиты информации в информационно-телекоммуникационных системах [Текст] / А. В. Аграновский, В. И. Мамай, И. Г. Назаров и др. — Ростов-на-Дону: СКНЦ ВШ, 2016. — 258 с.

2. Бржезинская А. Д. Создание политики информационной безопасности и ее влияние на процесс управления безопасностью [Текст] / А. Д. Бржезинская // Молодежный научный форум: Общественные и экономические науки. — 2016. — №11. — С. 231—235.

3. Гафнер В. В. Информационная безопасность [Текст] / В .В. Гафнер. – Ростов на Дону: Феникс, 2010. – 324 с.

4. Глобалтека — Дидактические требования к электронным учебникам [Электронный ресурс]. — Режим доступа: http://globalteka.ru/-order/13716.html (дата обращения: 31.10.2018).

5. Дронов Д. Р. Разработка политики безопасности предприятия, занимающегося разработкой программного обеспечения [Текст] / Д. Р. Дронов // Молодой ученый. — 2017. — №13. — С. 37—41.

6. Информационная безопасность [Электронный ресурс]. — Режим доступа: http://itsec.ru/articles2/Inf_security/ugrozy-bezopasnosti-web-portalov-i-metody-zaschity/ (дата обращения: 24.10.2018).

7. Информационная безопасность [Электронный ресурс]. — Режим доступа: https://www.securitylab.ru/news/tags/%E8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF+%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC// (дата обращения: 14.02.2019).

8. Информационная безопасность — дело государственной важности [Электронный ресурс]. — Режим доступа: https://www.security-lab.ru/analytics/489911.php/ (дата обращения: 24.10.2018).

9. Итоги 2017 года в сфере ИБ: угрозы, инциденты, тренды, события [Электронный ресурс]. — Режим доступа: https://www.securitylab.ru/blog/-personal/Informacionnaya_bezopasnost_v_detalyah/343228.php/ (дата обращения: 26.10.2018).

10. Код ИБ.АКАДЕМИЯ или база знаний безопасника [Электронный ресурс]. — Режим доступа: https://www.securitylab.ru/analytics/495697.php/ (дата обращения: 25.10.2018).

11. Марков А. С. Методы оценки несоответствия средств защиты информации [Текст] / А. С. Марков, В. Л. Цирлов, А. В. Барабанов. — под ред. А. С. Маркова. — Москва: Радио и связь, 2012. — 183 с.

12. Обзор методов защиты корпоративной информации — Информационная безопасность [Электронный ресурс]. — Режим доступа: http://itsec.ru/articles2/Inf_security/obzor-metodov-zaschity-korporativnoy-informatsii/ (дата обращения: 26.10.2018).

13. Петренко С. А. Политики безопасности компании при работе в Интернет [Текст]: / С. А. Петренко, В. А. Курбатов. — 3-е издание. — Москва: ДМК Пресс, 2018. — 397 с.

14. Продажа, обмен, выкуп и реализация тягачей и полуприцепов — лучшие условия продажи от компании Глобал Трак Сейлс [Электронный ресурс]. — Режим доступа: http://www.gt-sales.ru/about/ (дата обращения: 25.10.2018).

15. Секьюрити Лаб [Электронный ресурс]. — Режим доступа: https://www.securitylab.ru/analytics/487450.php/ (дата обращения: 25.10.2018).

16. Создание политики ИБ и ее влияние на процесс управления безопасностью — Информационная безопасность [Электронный ресурс]. — Режим доступа: http://www.itsec.ru/articles2/control/sozdanie-politiki-ib-i-ee-vliyanie-na-protsess-upravleniya-bezopasnostyu/ (дата обращения: 26.10.2018).

17. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (последняя редакция) / КонсультантПлюс [Электронный ресурс] — Ре-

жим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 04.02.2019).

18. Федеральный закон «О персональных данных» от 27.07.2006 № 152ФЗ (последняя редакция) / КонсультантПлюс [Электронный ресурс] — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 28.01.2019).

19. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) / КонсультантПлюс [Электронный ресурс] — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 29.01.2019).

20. Шайдуров А. А. Информационная безопасность и защита информации [Текст]: учебное пособие для вузов / А. А. Шайдуров. — Екатеринбург: Издательство РГППУ, 2010. — 129 с.

21. Шептура С. В. Курс по дисциплине «Информационная безопасность» [Текст]: учеб. пособие для вузов / С. В. Шептура. — Москва: Издательство МФПА, 2010 — 102 с.

22. Электронные учебники: рекомендации по разработке, внедрению и использованию интерактивных мультимедийных электронных учебников нового поколения для общего образования на базе современных мобильных электронных устройств [Текст] / Федеральный институт развития образования. — Москва: Федеральный институт развития образования, 2014. — 84 с

23. Эльконин Д. Б. Избранные психологические труды. Проблемы возрастной и педагогической психологии [Текст] / Д. Б. Эльконин. — под ред. Д. И. Фельдштейна. — Москва: Международная педагогическая академия, 2017. — 165 с.

24. Ялукова И. В. Электронный учебник как средство индивидуального подхода на уроках информатики [Текст] / Проблемы и перспективы развития образования: материалы V междунар. науч. конф. — Пермь: Меркурий, 2014. — С. 181—182.

25. Ярочкин В. И. Информационная безопасность [Текст]: учебник для вузов / В. И. Ярочкин. — Москва: Гаудеамус, 2009. — 544 с.

ПРИЛОЖЕНИЕ