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

ЭЛЕКТРОННОЕ ПОСОБИЕ «ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕНЕДЖЕРОВ ТОРГОВОЙ КОМПАНИИ»

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: 135

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

ЭЛЕКТРОННОЕ ПОСОБИЕ «ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕНЕДЖЕРОВ ТОРГОВОЙ КОМПАНИИ»

Исполнитель:
обучающийся группы № ЗИБ-501 М. А. Завьялов
Руководитель:
старший преподаватель Т. П. Телепова

Нормоконтролер: С. Ю. Ярина

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из электронного пособия «Организация информационной безопасности» для менеджеров группы компаний «Союзоптторг» и пояснительной записки на 59 страницах, содержащей 25 рисунков, 33 источника литературы, а также 1 приложение на 2 страницах.

Ключевые слова: ТОРГОВАЯ ОРГАНИЗАЦИЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ЭЛЕКТРОННОЕ ПОСОБИЕ

Завьялов М. А., Электронное пособие «Организация информационной безопасности менеджеров торговой компании»: выпускная квалификационная работа / М. А. Завьялов; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 59 с.

В работе рассмотрены вопросы, связанные с дополнительной подготовкой менеджеров по продажам в области информационной безопасности.

Целью работы является разработка электронного пособия для самоподготовки к тестированию на курсах дополнительной подготовки менеджеров по продажам Группы компаний «Союзоптторг».

Для достижения цели были поставлены задачи: рассмотреть теоретические основы обеспечения информационной безопасности в торговле; провести анализ деятельности компании, ее структуру, информационные ресурсы и выявить задачи, решение которых повышает информационную безопасность в работе менеджеров; разработать структуру электронного пособия и отобрать информацию, необходимую для подготовки менеджеров по продажам к тестированию на курсах дополнительной подготовки; разработать электронный вариант пособия.

Электронное пособие помогает менеджерам торговой компании повысить уровень подготовки в области информационной безопасности и качество выполняемых профессиональных задач.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Проникновение информационно-коммуникационных технологий во все сферы жизнедеятельности человека и общества повлекло как положительные, так и отрицательные последствия. Компьютеризация и информатизация торговых организаций позволила ускорить взаимодействие между менеджерами, а также оптимизировать их работу. Однако наряду с увеличением скорости работы появилась проблема информационной безопасности деятельности торговых компаний. Особенно актуально соблюдение информационной безопасности в торговых компаниях с большим территориальным масштабом, с охватом городов, регионов и стран, в которых реализованы распределённые компьютерные и информационные системы и осуществляются соответствующие политики информационной безопасности. Информационная безопасность таких организаций заключается в защищенности информации от несанкционированного доступа, уничтожения, изменения и других действий. Доступ к конфиденциальной информации и ее изменение могут нанести существенный урон финансовому положению компании. В некоторых случаях даже хищение 1/5 конфиденциальной информации может иметь критические последствия для финансовой безопасности.

Причиной утечки информации или ее порчи, если отсутствует должное обеспечение информационной безопасности организации, могут быть различные случайности, вызванные неопытностью сотрудников и незнанием ими цели, роли информационной безопасности, угрозах, формах и методах защиты. Поскольку автор выпускной квалификационной работы является менеджером одной из торговых международных компаний, опыт его работы показал не достаточный уровень знаний основных положений теории информационной безопасности и недостаточную степень квалификации сотрудников в области ее практического соблюдения. Отсюда возникает про-

блема обучения менеджеров компании на курсах дополнительной подготовки в области информационной безопасности.

Знания основных понятий, умения соблюдать политику информационной безопасности предприятия или компании, эффективно реализовывать задачи по обеспечению информационной безопасности в профессиональной деятельности менеджеров обуславливают актуальность и определяют выбор темы выпускной квалификационной работы.

В связи с вышесказанным были определены объект и предмет выпускной квалификационной работы.

Объектом выпускной квалификационной работы является процесс дополнительной подготовки менеджеров по продажам в области информационной безопасности.

Предметом выпускной квалификационной работы является электронное пособие для самоподготовки менеджеров по вопросам информационной безопасности.

Цель данной работы — разработать электронное пособие для самоподготовки к тестированию на курсах дополнительной подготовки менеджеров по продажам группы компаний «Союзоптторг».

В соответствие с поставленной целью в работе определены следующие задачи:

1. Рассмотреть теоретические основы обеспечения информационной безопасности в торговле.

2. Провести анализ деятельности компании, ее структуру, информационные ресурсы и выявить задачи, решение которых повышает информационную безопасность в работе менеджеров.

3. Разработать структуру электронного пособия и отобрать информацию, необходимую для подготовки менеджеров по продажам к тестированию на курсах дополнительной подготовки.

4. Разработать электронный вариант пособия.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТОРГОВЛЕ

1.1 Анализ современного состояния информационной безопасности в торговле

1.1.1 Современные угрозы информационной безопасности в торговых компаниях

Современные тенденции развития торговли в России приводят к укрупнению компаний за счет увеличения численности предприятий в их составе, объединения небольших компаний в крупные, создания сетевых распределительных центров. В результате чего растут требования к информационным технологиям, к информационной безопасности в организациях торговли. Обработка информационных потоков в любой компании требует высоких темпов, абсолютной точности и конфиденциальности.

Внедрение информационных технологий в деятельность торговых организаций позволило ускорить взаимодействие между сотрудниками и клиентами, а также оптимизировало их работу. Однако наряду с увеличением скорости работы появились новые возможности и для недобросовестных сотрудников. Теперь они могут быстро и просто, не покидая своего рабочего места, передать конфиденциальную информацию третьему лицу.

Конфиденциальная для бизнеса информация входит в сферу повышенного интереса конкурирующих компаний. Для недобросовестных конкурентов, коррупционеров и других злоумышленников особый интерес представляет информация о составе менеджмента предприятий, их статусе и деятельности фирмы. Доступ к конфиденциальной информации, ее изменение могут нанести существенный урон финансовому положению компании [2].

Управление современным магазином, предприятием оптовой торговли и торговой сетью предполагает использование автоматизированных систем в комплексе для торгового, складского и бухгалтерского учета. Какова бы ни была структура фирмы, основные операции: ведение учета договоров, заключение контрактов, движение товарно-материальных ценностей, денежных средств и бухгалтерского учета должны осуществляться в едином информационном пространстве.

Для разработки концепции обеспечения информационной безопасности под информацией понимают сведения, которые доступны для сбора, хранения, обработки (редактирования, преобразования), использования и передачи различными способами, в том числе в компьютерных сетях и других информационных системах.

Ущерб информационным ресурсам может быть нанесен:

- осуществлением несанкционированного доступа и копирования конфиденциальной информации;
- подкупом сотрудников с целью получения доступа к конфиденциальной информации или информационным и ресурсам компании;
- путем перехвата информации, которая передается внутри информационной системы;
- путем подслушивания конфиденциальных переговоров, ведущихся в служебных помещениях, служебном и личном автотранспорте и т.д.

Основными источниками информации являются люди, документы, технические носители, технические средства, продукция.

Основными способами несанкционированного получения информации являются:

- разглашение конфиденциальной информации;
- несанкционированный доступ к информационным ресурсам;
- утечка конфиденциальной информации по вине сотрудников компании [27].

Аналитический центр InfoWatch опубликовал данные по утечке данных в России за 2016 год. Согласно исследованию, средства массовой информации обнародовали 213 случаев утечек информации из российских госорганов и компаний, что составляет 14 % от общемирового количества утечек. Самые частые случаи — это утечка платежной информации и персональных данных — 80 %.

В 68 % случаев виновными оказываются сотрудники организаций, и только в 8 % — руководство. По сравнению с 2015 годом количество утечек выросло на 89 %. На сегодня Россия занимает второе после США место в списке стран, наиболее сильно страдающих от утечек информации.

По результатам исследования причин угроз информационной безопасности можно выделить ряд проблем, которые представлены ниже.

Невнимательность и халатность сотрудников. Угрозу информационной безопасности компании, как ни странно, могут представлять вполне лояльные сотрудники и не помышляющие о краже важных данных. Непредумышленный вред конфиденциальным сведениям причиняется по простой халатности или неосведомленности работников. Всегда есть возможность того, что кто-нибудь откроет фишинговое письмо и внедрит вирус с личного ноутбука на сервер компании. Ни одна компания не застрахована от пересылки невнимательным сотрудником важных файлов не по тому адресу [10].

Использование пиратского программного обеспечения. Следует знать, что нелицензионные программы не дают защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Обладатель нелицензионного программного обеспечения (ПО) не получает технической поддержки, своевременных обновлений, предоставляемых компаниями-разработчиками. Вместе с ним он покупает и вирусы, способные нанести вред системе компьютерной безопасности. По данным исследования Microsoft, в 7 % изученных нелицензионных программ было найдено специальное программное обеспечение для кражи паролей и персональных данных.

DDoS-атаки (Distributed-Denial-of-Service — «распределенный отказ от обслуживания») — это поток ложных запросов от сотен тысяч географически распределенных хостов, которые блокируют выбранный ресурс одним из двух путей.

Первый путь — это прямая атака на канал связи, который полностью блокируется огромным количеством бесполезных данных. *Второй* — атака непосредственно на сервер ресурса. Недоступность или ухудшение качества работы публичных веб-сервисов в результате атак может продолжаться довольно длительное время, от нескольких часов до нескольких дней. Обычно подобные атаки используются в ходе конкурентной борьбы, шантажа компаний или для отвлечения внимания системных администраторов от неких противоправных действий вроде похищения денежных средств со счетов. По мнению специалистов, именно кражи являются основным мотивом DDoS-атак.

Вирусы. Одной из самых опасных на сегодняшний день угроз информационной безопасности являются компьютерные вирусы. Это подтверждается многомиллионным ущербом, который несут компании в результате вирусных атак. Если раньше атакам подвергались в основном серверы стандартных веб-служб, то сегодня вирусы способны воздействовать и на межсетевые экраны, коммутаторы, мобильные устройства, маршрутизаторы [10].

Угрозы со стороны совладельцев бизнеса. Именно легальные пользователи — одна из основных причин утечек информации в компаниях. Такие утечки специалисты называют инсайдерскими.

Законодательные перипетии. Государственные органы в России наделены правом конфисковать в ходе проверок оборудование и носители информации. Поскольку большая часть важных данных компании хранится в электронном виде на серверах, то в случае их изъятия компания на какое-то время просто останавливает свою деятельность. Простои при этом никто не компенсирует, а если проверка затягивается, большие убытки могут привести к прекращению деятельности фирмы. Изъятие оборудования — одна из ост-

рейших проблем современного бизнеса, при этом поводом для него может послужить все что угодно — от решения следователя до решения суда в рамках какого-либо уголовного дела [10].

1.1.2 Анализ методов и средств защиты информации в сетевых торговых компаниях

Сеть магазинов — это два или более торговых заведения, находящихся под общим владением и контролем, продающих товары аналогичного ассортимента, имеющих общую службу закупок и сбыта, а возможно аналогичное архитектурное оформление.

Преимущества сетевой торговли заключаются в следующем:

- с учетом территориальных сегментов целевого рынка возможно размещение товара с изменением пространства;
- в соответствии с потребительскими предпочтениями возможно изменение ассортимента товаров и формирование привлекательного ассортимента по конкурентоспособным ценам;
- размеры сетей позволяют им закупать большие партии товаров. получая при этом максимальные скидки и экономя на транспортных расходах;
- централизация и высокий уровень управления всей коммерческой деятельностью за счет привлечения квалифицированных специалистов позволяют избежать многих недостатков, характерных для отдельного магазина;
- возможна диверсификация видов деятельности с учетом повышения эффективности;
- снижение затрат на единицу товара за счет экономии на издержках по стимулированию сбыта, закупая рекламу, выгодную для своих магазинов, и относя расходы на большое количество товара;
- способность объединить функции оптовой и розничной торговли;

- сети дают своим магазинам определенную свободу, чтобы те могли с учетом местных потребительских предпочтений успешно вести конкурентную борьбу [24].

Розничная торговая сеть — это совокупность розничных торговых предприятий и других торговых единиц, размещенных на определенной территории с целью продажи товаров и обслуживания покупателей [23].

Розничная сеть представляет собой совокупность торговых предприятий, взаимодействующих на основе единого координирования, определяемого внешней средой. Эта сеть включает специально оборудованные здания (магазины), осуществляющие куплю-продажу товаров и оказание услуг покупателям для их личного, семейного и домашнего использования.

Специализированные розничные сети (в том числе и узкоспециализированные) реализуют одну группу товаров или часть товарной группы. Это позволяет предоставлять покупателям более глубокий и насыщенный ассортимент, иметь более тесные связи с поставщиками, сокращать оформление документации. В специализированных предприятиях имеются лучшие условия для изучения покупательского спроса, больше возможностей для предложения покупателям сервисных услуг. Представителями специализированных розничных сетей являются «М. Видео», «Эльдорадо», «Высшая лига», «Спортмастер», «Бибабо», «Позитроника», «Мир», «Эконика», «Техносила» [24].

Главными задачами любой системы информационной безопасности являются: обеспечение доступности данных для авторизированных пользователей, возможность оперативного получения информационных услуг; гарантия целостности информации, ее актуальность и защищенность от несанкционированного изменения или уничтожения; обеспечение конфиденциальности сведений. Для обеспечения защиты информации необходимо предпринимать следующие меры: формирование политики безопасности и составление соответствующей документации; внедрение защитных технических средств.

В сетевых компаниях, как правило, выделяют ряд средств информационной защиты. Рассмотрим их.

Физические средства защиты информации. К ним относятся ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами. Большое распространение получили HID-карты для контроля доступа. Например, при внедрении этой системы, пройти в серверную или другое важное подразделение компании могут лишь те, кому такой доступ предоставлен по протоколу.

Базовые средства защиты электронной информации. Это незаменимый компонент обеспечения информационной безопасности компании. К ним относятся многочисленные антивирусные программы, а также системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции. Корпоративные почтовые ящики обязательно должны быть оборудованы такими системами. Кроме того, необходима организация дифференцированного доступа к информации и систематическая смена паролей.

Анти-DDoS. Грамотная защита от DDoS-атак собственными силами невозможна. Многие разработчики программного обеспечения предлагают услугу анти-DDoS, которая способна защитить от подобных нападений. Как только в системе обнаруживается трафик необычного типа или качества, активируется система защиты, выявляющая и блокирующая вредный трафик. При этом бизнес-трафик поступает беспрепятственно. Система способна срабатывать неограниченное количество раз, до тех пор, пока угроза не будет полностью устранена.

Резервное копирование данных. Это решение подразумевает хранение важной информации не только на конкретном компьютере, но и на других устройствах: внешнем носителе или сервере. В последнее время особенно актуальной стала услуга удаленного хранения различной информации в «облаке» дата-центров. Именно такое копирование способно защитить компанию в

случае чрезвычайной ситуации, например, при изъятии сервера органами власти.

Шифрование данных при передаче информации в электронном формате (end-to-end protection). Чтобы обеспечить конфиденциальность информации при ее передаче в электронном формате применяются различные виды шифрования. Шифрование дает возможность подтвердить подлинность передаваемой информации, защитить ее при хранении на открытых носителях, защитить ПО и другие информационные ресурсы компании от несанкционированного копирования и использования.

Таким образом, защита информации должна осуществляться комплексно, сразу по нескольким направлениям. Чем больше методов будет задействовано, тем меньше вероятность возникновения угроз и утечки, тем устойчивее положение компании на рынке [10].

Надежную защиту информации может обеспечить только комплексный подход, подразумевающий одновременное использование аппаратных, программных и криптографических средств (ни одно из этих средств в отдельности не является достаточно надежным). Такой подход включает детальный анализ внедряемой системы, оценку угроз безопасности, изучение средств, используемых при построении системы, и их возможностей, анализ соотношения внутренних и внешних угроз и оценку возможности внесения изменений в систему [6].

Сложность создания системы защиты информации в территориально-распределенной компании определяется тем, что данные могут быть похищены из компьютера и одновременно оставаться на месте; ценность некоторых данных заключается в обладании ими, а не в уничтожении или изменении. Специалист в области безопасности информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности накопленной в организации информации. В его функции входит обеспечение физической (технические средства, линии связи и удаленные

компьютеры) и логической (данные, прикладные программы, операционная система) защиты информационных ресурсов [4].

В больших и малых компаниях, фирмах, организациях для создания единой информационной системы используется локальная сеть. Она служит для связи рабочих станций пользователей, серверов, рабочих мест администраторов, коммуникационного оборудования, сетевых принтеров и другого оборудования.

При наличии филиалов (удаленных пользователей) особенно необходимы межсетевые экраны, позволяющие организовать защиту сегмента локальной сети от глобальной сети, которая используется как транспорт для взаимодействия удаленных локальных сегментов (VPN). Кроме того, межсетевые экраны контролируют входную информацию из открытой сети (фильтрация сервисов). Межсетевые экраны дополняются ДМЗ — демилитаризованной зоной, в которой установлены серверы почты, Веб-серверы, которые принимают на себя удар вирусных и сетевых атак. Этот традиционный набор считается защитой локальной сети. Однако в действительности это может не быть защитой, если не реализованы некоторые основные принципы защиты информации.

В системе должна быть единая *политика безопасности*, которая определяет правила обращения с информацией так, чтобы исключить или снизить угрозы ущерба. Единая политика нужна, чтобы исключить противоречия между правилами обращения с одной и той же информацией в разных подразделениях организации.

Как минимум необходимо организовать *защиту целостности информационных ресурсов* от модификации или уничтожения. Идентификация и аутентификация, правила разграничения доступа, аудит и защита целостности должны реализовываться механизмами защиты [8].

Идентификация — это процедура распознавания субъекта по его идентификатору. Например, это определение имени, логина или номера.

Идентификация выполняется при попытке войти в какую-либо систему (например, в операционную систему или в сервис электронной почты). После идентификации производится аутентификация:

Аутентификация — это процедура проверки подлинности. Пользователя проверяют с помощью пароля, письмо проверяют по электронной подписи или другим способами.

Если определили идентификатор, подтвердили подлинность, то можно предоставить и доступ, то есть, выполнить авторизацию.

Авторизация — это предоставление доступа к какому-либо ресурсу (например, к электронной почте) [5].

Аудит информационной безопасности — это независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций.

Аудит позволяет получить наиболее полную и объективную оценку защищенности информационной системы, локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения информационной безопасности организации. В рамках аудита или отдельным проектом может быть проведен тест на проникновение, позволяющий проверить способность информационной системы компании противостоять попыткам проникновения в сеть и неправомочного воздействия на информацию [1].

На каждом рабочем месте и на серверах установлены операционные системы, которые, как правило, обладают набором механизмов защиты, обеспечивающих идентификацию и аутентификацию, разграничение доступа, аудит на данном компьютере.

Основными механизмами защиты целостности являются резервное копирование (backup), электронно-цифровая подпись (ЭЦП) и коды аутентификации. Однако реализация политики безопасности на отдельном компьютере не может означать, что выполняется единая политика безопасности во всей системе.

Например, пользователи по сети могут обращаться на файловый сервер для получения необходимой информации или отправки документов в файле на печать на сетевой принтер. Обращение на сервер предполагает копирование файла из одного компьютера, где файл находится под защитой локальной политики безопасности и средств ее поддержки, в другой компьютер, на котором действует локальная политика безопасности и механизмы ее поддержки.

Очевидно, что передача файла или информации из этого файла в файл на другой рабочей станции не управляется локальной политикой безопасности, т. е. должны быть механизмы реализации политики безопасности системы в целом, с помощью которых может быть разрешен доступ субъекта на одной машине к информации, расположенной на другой машине.

В частности, для такого доступа субъект из рабочей станции 1 (PC1), запрашивающий доступ к информации на компьютере PC2, должен быть идентифицирован и аутентифицирован на PC2, т. е. его аутентификационная информация (пароль) на PC1 должна быть передана на PC2. Этот субъект должен быть учтен на PC2 в матрице разграничения доступа, а его действия должны отслеживаться аудитом на PC1 и PC2. Так как в сегменте локальной сети передача является широковещательной, то передача пароля для аутентификации на PC2 может быть подслушана на любой рабочей станции и в следующий раз подслушивающий субъект сможет запрашивать информацию на другой машине от чужого имени.

Чтобы контролировать сеть, необходим мониторинг сети. Он решает две задачи — контроль действий администратора сети и аудит сети.

Для исключения подслушивания вместо концентраторов надо по возможности использовать коммутаторы. Коммутаторы частично решают задачу разграничения доступа в сети. Если успешно защититься от подслушивания и обращения от чужого имени, тогда концентрация на серверах информации для реализации дискреционной политики в сети позволяет поддерживать сетевое разграничение доступа.

Кроме того, большой проблемой для информационных систем российских компаний являются не столько внешние атаки, сколько собственный персонал. Действия неквалифицированных специалистов часто становятся причиной тяжелых последствий. Хотя основной задачей системы информационной безопасности является обеспечение постоянной доступности защищаемых ресурсов для легальных пользователей, и полная недоступность для нелегальных, также необходим и постоянный контроль действий легальных пользователей.

Любая политика информационной безопасности должна отвечать следующим требованиям:

- интегрированность (все элементы, из которых она состоит, должны подходить и дополнять друг друга);
- комплексность (использование программного обеспечения для защиты в комплексе);
- достаточность (нет необходимости усложнять управление системой безопасности).

Исходя из вышесказанного, можно предложить схему практической реализации системы защиты распределенной компьютерной сети организации, на которой показаны следующие основные элементы системы:

- авторизация и разграничение;
- шифрование данных;
- межсетевые экраны с поддержкой VPN;
- система аудита и защиты от атак и антивирусная защита;
- автоматизация делопроизводства [8].

Общая модель построения системы информационной безопасности

Систему информационной безопасности можно определить как организованную совокупность органов, средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа к ней. Для построения концептуальной модели информационной безопасности не зависимо от того насколько простая или сложная у Вас ин-

формационная система, необходимо как минимум ответить на три вопроса: что защищать, от кого защищать и как защищать [16].

На рисунке 1 схематично представлена общая модель информационной безопасности торговой компании.

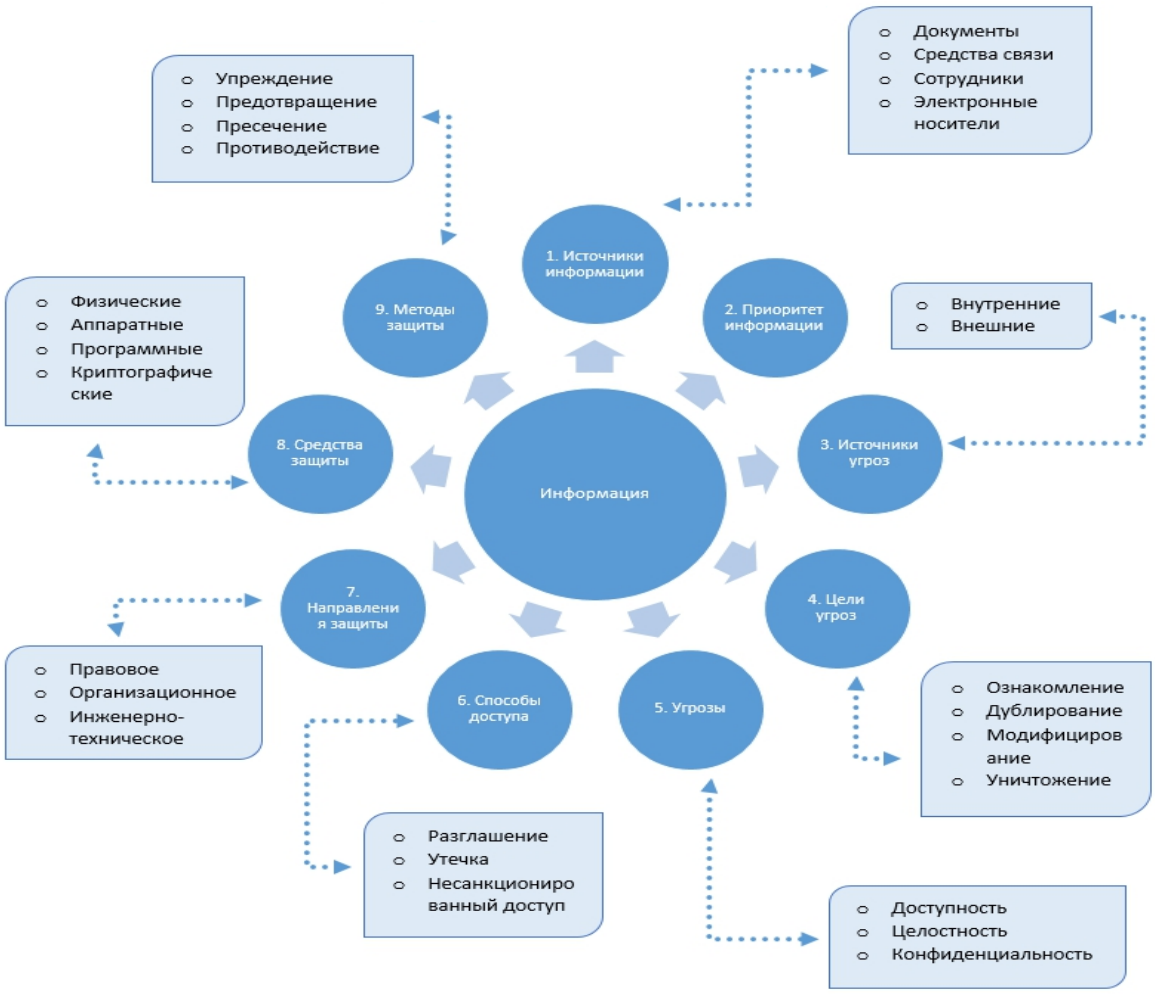

Рисунок 1 — Модель информационной безопасности

В ней можно выделить следующие пункты:

1. Источники информации.
2. Приоритет информации.
3. Источники угроз.
4. Цели угроз.
5. Угрозы.
6. Способы доступа.
7. Направления защиты.

8. Средства защиты.
9. Методы защиты.

*Основными источниками информации являются***:** люди, документы, публикации, технические носители, технические средства, продукция и отходы.

Основными способами несанкционированного получения информации являются:

- разглашение конфиденциальной информации;
- несанкционированный доступ к информационным ресурсам;
- утечка конфиденциальной информации по вине сотрудников компании.

Руководители компаний должны осознать важность информационной безопасности, научиться предвидеть будущие тенденции и управлять ими. Эффективная работа систем безопасности должна стать первоочередной задачей для всего предприятия в целом [16].

Целью защиты информации является сведение к минимуму потерь в управлении, вызванных нарушением целостности данных, их конфиденциальности или недоступности информации для потребителей.

Рассмотрим основные направления защиты информации.

Правовая защита включает: Законодательство РФ, собственные нормативно-правовые документы, в том числе: положение о сохранении конфиденциальной информации, перечень сведений, составляющих коммерческую тайну, инструкция о порядке допуска сотрудников к конфиденциальной информации, положение о делопроизводстве и документообороте, обязательство сотрудника о неразглашении конфиденциальной информации, памятка сотруднику о сохранении коммерческой тайны и др.;

Организационная защита включает режимно-административные и организационные мероприятия. К ним относятся: организация службы безопасности, организация внутриобъектового и пропускного режимов, организация работы с сотрудниками по неразглашению сведений, составляющих

коммерческую и служебную тайну, организация работы с документами, организация работы по анализу внешних и внутренних угроз и пр.

Инженерно-техническая защита — предусматривает применение различных технических, электронных и программных средств, предназначенных для защиты информации.

Количество стандартов и спецификаций, включая международные, национальные и отраслевые в области информационной безопасности бесконечно, приведем только некоторые из них, полный список национальных стандартов предоставлен на сайте ФСТЭК России в соответствующем разделе «Национальные стандарты».

1.2 Анализ литературы и интернет-источников

1.2.1 Анализ литературы

Для разработки учебного пособия необходимо выполнить обзор и анализ литературы и интернет-источников по темам «Информационная безопасность», «Защита информации», что позволит понять теоретическую сторону исследуемой темы и систематизировать материал.

В книге Ю. Родичева «Нормативная база и стандарты в области информационной безопасности. Учебное пособие» рассмотрены наиболее важные нормативные документы ФСТЭК, а также международные и национальные стандарты Российской Федерации в области информационной безопасности.

Предназначено дня студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности, слушателей курсов повышения квалификации по проблемам зашиты информации. Рассмотренные вопросы будут полезны руководителям учреждений, а также специалистам в области информационных технологий, занимающимся разра-

боткой и эксплуатацией аппаратно-программных средств и обеспечением их безопасности.

В книге С. А. Нестерова «Информационная безопасность: учебник и практикум для СПО» системно излагаются теоретические основы информационной безопасности и описываются практические аспекты, связанные с их реализацией. В пособии рассматриваются теоретические основы защиты информации, основы криптографии, защита информации в IP-сетях, анализ и управление рисками в сфере информационной безопасности. Теоретический материал сопровождается лабораторными работами, выделенными в отдельный раздел.

Учебник может использоваться с целью повышения квалификации в рамках образовательной программы дополнительного профессионального образования «Информатика и вычислительная техника». Также оно может быть полезно широкому кругу специалистов в области информационных технологий.

В книге авторов О. В. Казарина и А. С. Забабурина «Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для вузов» рассматриваются организационно-технические и нормативно-правовые аспекты разработки и эксплуатации программ, в том числе процесс сертификации программных комплексов по требованиям безопасности информации.

Цель учебника — овладение теоретическими знаниями и формирование практических умений и навыков в области обеспечения безопасности программного обеспечения, в том числе освоение комплекса мер, методов и способов защиты программ от различного рода деструктивных угроз в процессе их возникновения и реализации в современных информационных системах. Для успешного освоения материалов учебника в приложении приведены краткий терминологический словарь, сведения, необходимые для подготовки студентов к практическим занятиям, для выполнения лабораторных работ, а также для организации самостоятельной работы.

Учебное пособие «Защита информации техническими средствами» под редакцией Ю. Ф. Каторина посвящено теме борьбы с промышленным шпионажем. Авторы в простой и доступной форме излагают основные способы съёма конфиденциальной информации с помощью технических средств и принципы построения средств и систем защиты. Пособие предназначено для формирования у студентов знаний по основам инженерно-технической защиты информации, а также развития в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации. В полном объёме излагаемый материал рассчитан для подготовки студентов технических университетов по направлению: 090900 — «Информационная безопасность» и 090103 — «Организация и технология защиты информации».

В учебном пособии «Теория информационной безопасности и методология защиты информации» Л. В. Астаховой рассмотрены основные теоретико-методологические вопросы информационной безопасности и защиты информации: понятия информационной безопасности и защиты информации, структура и содержание угроз защищаемой информации, виды, методы и средства защиты информации, ресурсное обеспечение защиты информации. Учебное пособие рассчитано на студентов, изучающих дисциплину «Теория информационной безопасности и методология защиты информации», включенную в базовую часть профессионального цикла дисциплин ФГОС-3 по специальности 090915 «Безопасность информационных технологий в правоохранительной сфере». Также оно может быть полезно студентам, изучающим дисциплину «Основы информационной безопасности» в рамках других направлений, связанных с защитой информации: 090900 «Информационная безопасность», 090303 «Информационная безопасность автоматизированных систем» и др.

В учебном пособии «Основы информационной безопасности» авторов Ю. А. Гатчина, Е. В. Климовой рассматривается законодательная база информационной безопасности, приводится перечень возможных угроз. Отра-

жены основные подходы к созданию систем защиты информации и представлена классификация мер по обеспечению безопасности компьютерных систем.

Пособие предназначено для студентов, специализирующихся в области информационной безопасности (специальность 090104 — Комплексная защита объектов информатизации, дисциплина «Теория информационной безопасности и методология защиты информации) и слушателей факультета повышения квалификации.

Целью данного учебного пособия является ознакомление студентов с основами информационной безопасности компьютерных систем, проблемами защиты информации и подходами к их решению [6].

Учебное пособие «Информационная безопасность и защита информации» авторов Е. К. Барановой и А. В. Бабаш посвящено рассмотрению базовых вопросов информационной безопасности и защиты информации и может быть рекомендовано бакалаврам и магистрам, изучающим курсы «Информационная безопасность» и «Управление информационной безопасностью», а также смежные с ними дисциплины. Книга может быть также полезна аспирантам и специалистам, интересующимися вопросами защиты информации.

С развитием локальных и глобальных сетей удаленные атаки становятся лидирующими как по числу попыток, так и по успешности их реализации. Специфика распределенных вычислительных систем состоит в том, что, если в локальных вычислительных сетях наиболее часты угрозы конфиденциальности и целостности информации, то в территориально-распределенных сетях на первое место выходит угроза нарушения доступности информации. Эти и другие вопросы рассмотрены в учебном пособии [2].

Вывод: учебников и учебных пособий на данную тему достаточно много, но в большинстве из них описываются базовые вопросы и методы их решений, в свою очередь в каждой определенной области деятельности (бизнес, банк, торговля и т.д.) имеются свои особенности и отличия.

1.2.2 Анализ интернет-источников

Интернет-источники предоставляют более конкретную информацию по исследуемой теме. В настоящее время информация актуальна и постоянно появляются новые статьи публикации, связанные с реализацией защиты информации в разных областях деятельности, авторы делятся опытом и предлагают свои разработки, а также много компаний, предоставляющих свои услуги в этой области.

Сайт Международной торговой палаты — Всемирная организация бизнеса (ICC) предлагает ряд статей «Обеспечение информационной безопасности организации», «Электронная коммерция в международной торговле», «Международное пиратство» и др. [18].

Сайт «Торговля и безопасность» предлагает ряд публикаций специалистов в разных областях, связанных с защитой информации: специалист по обеспечению качества программного обеспечения, сотрудник экспертного отдела, руководитель направления информационной безопасности компании и т.д. Авторы статей делятся опытом, рассказывая о реальных проблемах и решениях в компаниях [29].

В большинстве рассматриваемых интернет-источников предлагается обзор существующих проблем на примере реальных предприятий и компаний. В каждой компании используется свой специфичный для работы пакет программного обеспечения и средства защиты. То есть информация, предоставляемая интернет-источниками полезна, но не всегда можно ее применить в работе конкретной компании, зато можно проанализировать и выявить ошибки в существующей системе безопасности, и в итоге определиться с внесением необходимых изменений.

1.2.3 Анализ существующих электронных пособий для менеджеров торговых компаний

Учебные пособия по теме «Информационная безопасность и защита информации» в основном разрабатываются для студентов, изучающих данный курс в высших учебных заведениях, но не для системных администраторов конкретных компаний и организаций. Это связано с особенностями области деятельности и программным обеспечением конкретной компании. Невозможно создать универсальное учебное пособие.

Любая компания должна озаботиться этой проблемой и разработать пакет технической документации по информационной безопасности. Примерами таких документов могут служить «Политика управления паролями», «Политика управления доступом к ресурсам корпоративной сети», «Политика обеспечения безопасности при взаимодействии с сетью Интернет» и т.п.

Большинство организаций не располагают собственными людскими ресурсами, необходимыми для квалифицированной разработки и внедрения политик безопасности. Отыскать готовые политики безопасности, которые бы оказались применимыми в организации, соответствовали бы ее структуре и требованиям безопасности нереально. Несмотря на доступность соответствующих, в основном англоязычных, ресурсов в сети Интернет, они зачастую являются непригодными для практического использования [14].

Если компания предоставляет возможность пользователю зарегистрироваться на сайте и пользоваться возможностями сервиса, то обязательным является разработка Руководства пользователя по работе в «Личном кабинете» с правилами работы и обзором сервисов.

Менеджер по продажам — это сотрудник, которому необходимо самостоятельно принимать решения, действовать быстро и адекватно реагировать на ситуацию. Набор компетенций зависит от конкретной позиции, от того, в какой компании человек работает и какие продукты предлагает. Он при-

зван осуществлять связь между покупателями и торговыми и производящими организациями.

Трудовые обязанности менеджера:

- разрабатывает и обеспечивает реализацию мероприятий по организации и созданию сети сбыта товаров (разработка и построение каналов движения товаров к потребителям; построение отношений с оптовыми и розничными торговыми предприятиями, иными посредниками; развитие дилерских отношений);
- организует преддоговорную работу (выбор вида договоров: дистрибьюторский, купли-продажи; определение способов и форм исполнения обязательств, разработка преддоговорной документации, согласование разногласий, анализ документации покупателей) и заключает договоры (купли-продажи, поставки);
- создает и обеспечивает постоянное обновление информационных баз о покупателях (организационно-правовые формы, адреса, реквизиты, номера телефонов, фамилии руководителей и ведущих специалистов, финансовое состояние, объемы закупок, объемы продаж, своевременность и полнота исполнения обязательств).

То есть менеджер является активным пользователем информационной системы компании, он должен уверенно пользоваться специфичными для своей области деятельности программными продуктами, но, не забывая о правилах и требованиях политики безопасности, касающихся его сфер деятельности. Например, работа в электронной почте, работа с внешними носителями, организация доступа к информационным ресурсам и т.д.

Чтобы новому сотруднику легче было внедриться в работу, проводятся обучающие тренинги и занятия, по наиболее важным программам разработаны руководства или методические пособия. Но для отдельных категорий сотрудников практически не разрабатываются учебные пособия по правилам и требованиям политики безопасности.

Например, в процессе поиска информации по данной теме были найдены: инструкция пользователя по обеспечению информационной безопасности автоматизированного рабочего места, выделенного для обработки конфиденциальной информации (персональных данных); инструкция обеспечения информационной безопасности при использовании персональных компьютеров, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет» для сотрудников колледжа и общеобразовательной школы.

Исходя из этого, можно сделать *вывод*, что разработка электронного пособия по организации информационной безопасности для менеджеров торговой компании, актуальна.

2 ОПИСАНИЕ ЭЛЕКТРОННОГО ПОСОБИЯ ПО ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕНЕДЖЕРОВ ТОРГОВОЙ КОМПАНИИ

2.1 Описание группы компании «Союзоптторг»

Группа компаний «Союзоптторг» — один из ведущих дистрибьюторов пищевых ингредиентов в России и странах СНГ. Уже более 18 лет успешного сотрудничества с крупнейшими отечественными производителями продуктов питания. Компания предлагает более 2000 наименований продуктов и добавок от ведущих мировых производителей. Предлагаемые основные группы ингредиентов: улучшающие внешний вид, изменяющие структуру и физико-химические свойства, влияющие на вкус и аромат, замедляющие микробную и окислительную порчу пищевых продуктов. Осуществляются поставки из 23 стран мира: Аргентина, Китай, Италия, Колумбия, Нидерланды, Бразилия, Новая Зеландия, Япония, Индонезия и др.

Технологическая поддержка клиентов:

- помощь в организации технологического процесса (от подбора ингредиентов до контроля качества конечной продукции);
- поиск индивидуальных технологических решений; участие в разработке новых продуктов;
- проведение семинаров и обучающих тренингов для технологов предприятий;
- совместные производственные проекты с поставщиками
- выезд технологов компании на предприятие для проведения пробной выработки.

Группа компаний «Союзоптторг» (ГК) предлагает конкурентоспособные цены за счет заключения долгосрочных договоров с поставщиками и осуществления закупок в больших объёмах.

Компания представляет собой масштабную сеть филиалов в России и странах СНГ: центральный офис находится в Санкт-Петербурге; 13 филиалов в Москве, Краснодаре, Екатеринбурге, Омске, Новосибирске, Казани, Самаре, Павлодаре, Алматы, Киеве, Ташкенте, Минске, Даугавпилсе. Удобная налаженная оптимизированная работа с клиентами (CRM-система). ГК «Союзоптторг» гарантирует высокое качество всех поставляемых пищевых ингредиентов.

Ответственный подход к выбору партнёров: представители регулярно посещают предприятия поставщиков для отслеживания организации контроля качества продукции, эффективности логистики, безопасности производственного процесса. Производственная площадка ГК «Союзоптторг» — ООО «Пищевая производственная инициатива» — располагается в Санкт-Петербурге. В настоящий момент здесь выпускается несколько высокотехнологичных комплексных ингредиентов: Greengel Aqua и Greengel Fruit, смеси на основе гелланновой камеди для производства напитков и термостабильных начинок. С информацией о компании можно ознакомиться на сайте (рисунок 2).

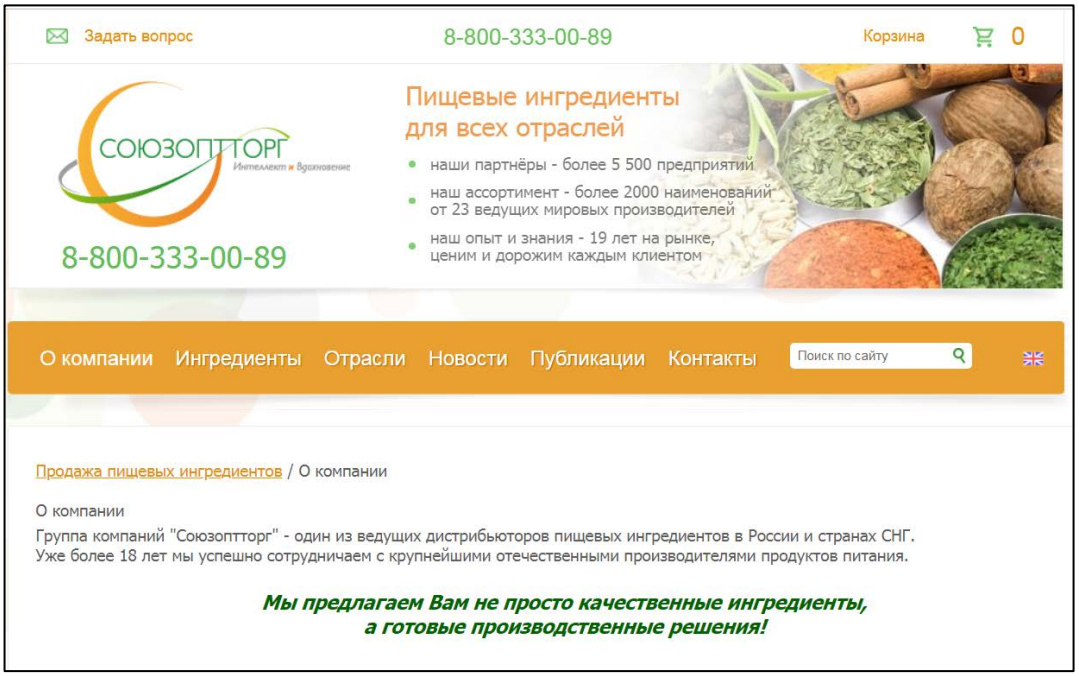

Рисунок 2 — Сайт группы компаний «Союзоптторг»

На рисунках 3 и 4 представлены обобщенные организационные схемы компании и филиала.

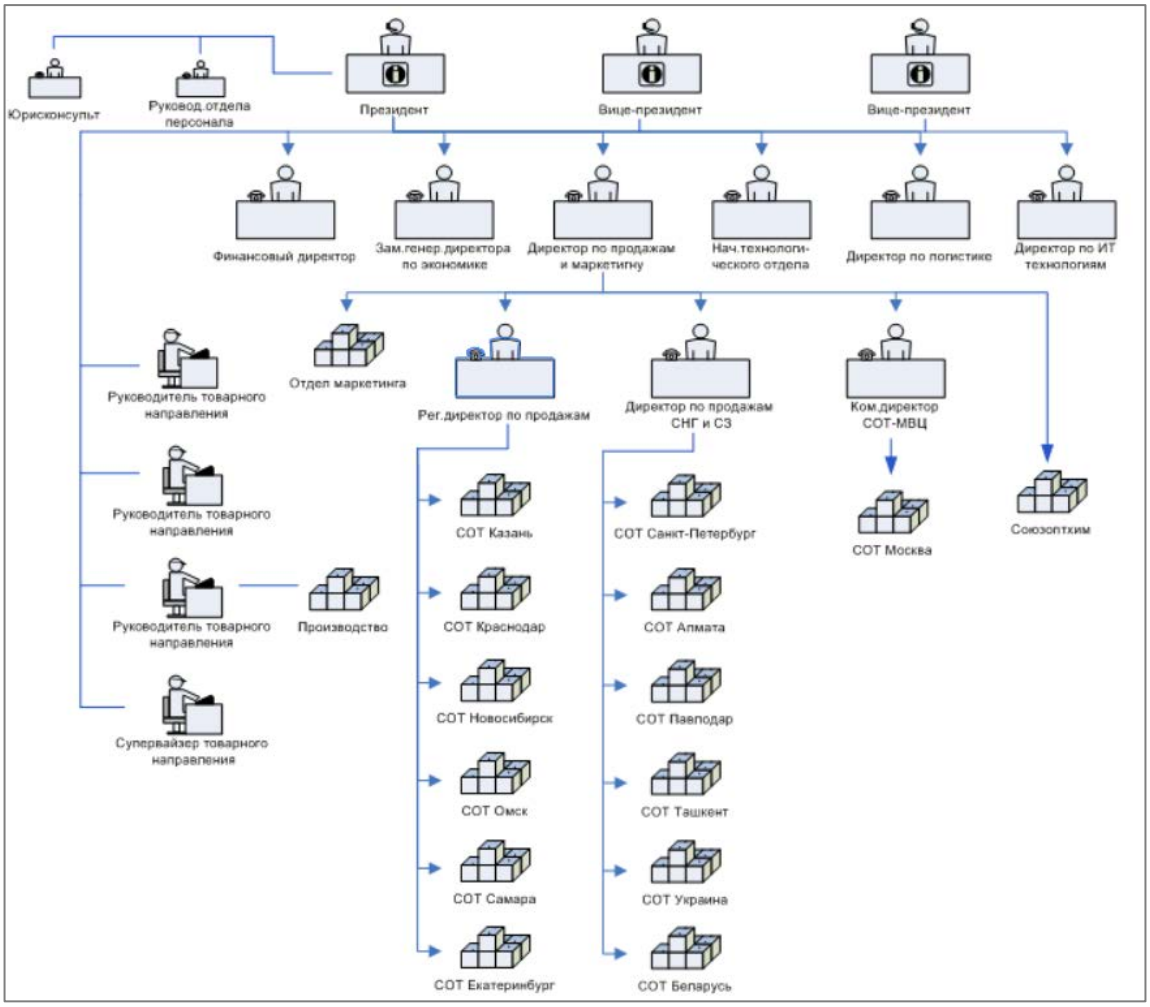

Рисунок 3 — Общая организационная схема торговой компании

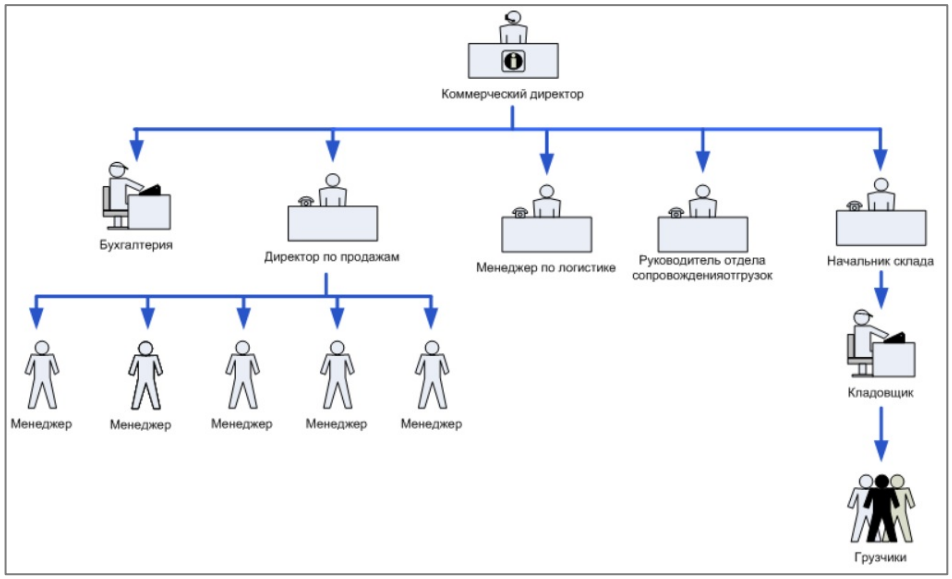

Рисунок 4 — Организационная схема филиала торговой компании

Администратор информационной безопасности и сотрудники IT-отдела достаточно тесно работают с персоналом компании. При небольшом количестве компьютеров этим обычно занимается сам администратор, в других случаях за каждым специалистом по информационной безопасности закрепляется определенный участок. Поэтому каждый такой ответственный хорошо знаком со своими «подопечными», знает их психологические характеристики и поведенческие характеристики.

Пренебрежение сотрудников техникой безопасности — проблема не инструктажей как таковых, а подачи. Если при устройстве на работу человеку дают на подпись формальный документ, то и отношение к нему будет формальным. Совсем иное — очный инструктаж, когда сотрудник компании рассказывает новичку, как вести себя в тех или иных случаях, и приводит примеры оплошности, которые не стоит повторять. Кроме вводных полезно практиковать дополнительные инструктажи (в случае выявления нарушений, как для виновника инцидента, так и для всего штата), а также периодические инструктажи, чтобы персонал не забывал о важности соблюдения правил.

Имеет смысл готовить и печатные или электронные материалы, чтобы люди могли обратиться к ним, когда возникнет необходимость.

Еще одно слабое звено в этой цепочке — отсутствие контроля усвоения информации. Проводить тестирование полезно как по результатам обучения, так и внепланово для всего персонала: постоянные проверки (и вероятность проведения новых без предупреждения) будут держать команду в тонусе. И, конечно, нельзя забывать про ответственность. Проверки ради проверок не имеют смысла: сотрудники должны осознавать, что несоблюдение правил чревато взысканиями.

Разрабатываемое пособие предназначено для менеджеров по продажам ГК «Союзоптторг» для самостоятельной подготовки к проверке знаний в области информационной безопасности компании.

Описание информационных ресурсов компании

В качестве информационных ресурсов мы рассматриваем используемое программное обеспечение, базы данных. Содержание информационных ресурсов компании представлено на рисунке 5.

Рисунок 5 — Содержание информационных ресурсов компании

Основной сервер компании расположен в главном офисе в Санкт-Петербурге. Там же находится IT-отдел. Администратор информационной безопасности и сотрудники IT-отдела достаточно тесно работают с персоналом компании. При небольшом количестве компьютеров этим обычно занимается сам администратор, в других случаях за каждым специалистом по информационной безопасности закрепляется определенный участок.

Программное обеспечение сервера. В филиалах реализованы локальные вычислительные сети с выходом в Интернет.

Программное обеспечение локальной сети отдела продаж

Менеджеры отдела продаж работают с большим количеством программ, как в сетевом, так и в локальном режимах. Менеджеры работают с такими программами: Outlook Web App, Skype, CRM-Система «КлиентКоммуникатор» (клиентская часть), 1С: Предприятие, MS Word, MS Excel и др. В качестве антивирусной программы используется Kaspersky Endpoint Security для Windows. Доступ к информации предоставляется в соответствии с разграничением прав в зависимости от должности. При увольнении все предо-

ставленные сотруднику права доступа к информационным ресурсам удаляются. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

Права у каждого отдельно взятого менеджера могут отличаться в связи с объемом работ, областями деятельности и регионами расположения клиентов менеджера.

Любые изменения прав и доступа менеджеров к информационным ресурсам производятся в установленном порядке, согласно регламента предоставления доступа. Каждому менеджеру любого филиала предоставляется персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать с информационными ресурсами (рисунок 6). В случае производственной необходимости некоторым менеджерам могут быть сопоставлены *несколько* учётных записей. Запрещено использовать общую пользовательскую учётную запись для группы пользователей.

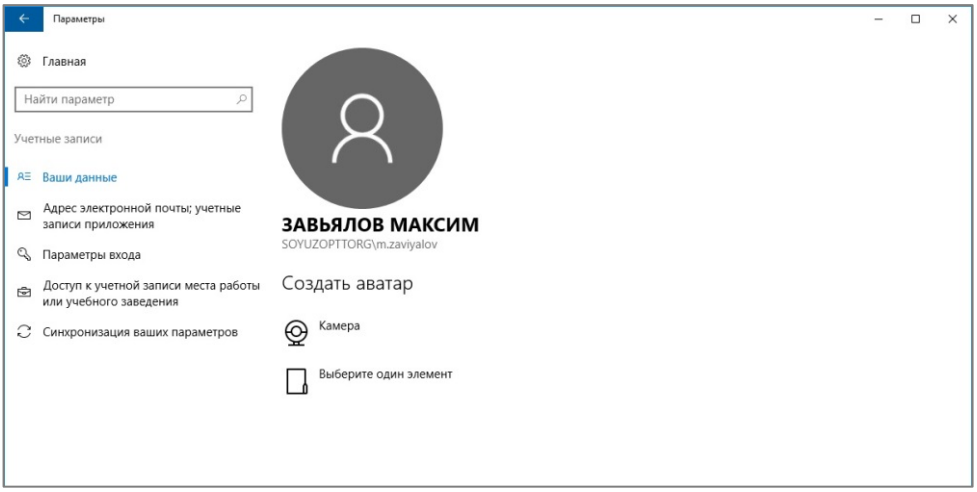

Рисунок 6 — Учетная запись менеджера в операционной системе Windows

В исключительных случаях, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), необходимо делать отметку в журнале учёта машинного времени, которая должна однозначно идентифицировать текущего пользователя учётной записи. Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено.

Анализ деятельности компании, ее организационной и информационной системы позволил выделить основные ***задачи информационной безопасности***, решение которых повлияет на повышение безопасной работы менеджеров по продажам каждого филиала компании:

- необходимость знаний основных понятий в области информационной безопасности и сведений по ее организации (политика безопасности, права доступа, вирусы и пр.);
- наличие различных прав доступа к информации и политики управление паролями;
- необходимость знаний своих обязанностей менеджерами при работе с документами, а также связанные с использованием и обработкой информационных ресурсов компании (базой данных, программным обеспечением);
- сформированность умений по соблюдению информационной безопасности при использовании информационных ресурсов локальной сети и сети Интернет**,** предотвращение угроз;
- сформированность умений безопасной эксплуатации программных средств обработки информации, используемых в компании.

2.2 Организация курсов дополнительной подготовки менеджеров по продажам компании

Основными пользователями информации и информационных ресурсов являются *менеджеры отдела продаж*. Все менеджеры по продажам компании должны проходить периодическую подготовку в области политики и процедур информационной безопасности, принятых в компании. Обучение менеджеров компании проводится *по двум основным направлениям*:

- формирования практических умений и навыков в соответствии с выполняемой работой, повышение ее эффективности;
- формирования знаний в области информационной безопасности, реализуемой в компании, повышения качества работы менеджеров.

Задачи, которые решаются на курсах дополнительной подготовки менеджеров при формировании практических умений и навыков в соответствии с выполняемой работой:

- изучение порядка организации труда на рабочих местах; требований делопроизводства;
- приобретение практических навыков в выполнении основных профессиональных функций и работы с документацией.

Задачи, которые решаются на курсах дополнительной подготовки менеджеров при формировании знаний в области информационной безопасности, реализуемой в компании, заключаются в формировании знаний и умений:

- основных понятий в области информационной безопасности и сведений по ее организации (в том числе по организации различных прав доступа к информации и формированию безопасных паролей);
- по соблюдению правил информационной безопасности при работе с документами и информационными ресурсами компании, решение проблемных ситуаций.
- по соблюдению информационной безопасности при использовании информационных ресурсов локальной сети и сети Интернет (особенности работы с корпоративной почтой), предотвращение угроз;
- безопасной эксплуатации программных средств обработки информации, используемых в компании.

Описание организации курсов дополнительной подготовки

Курсы обучения проходят в городе Санкт-Петербург, где находится головной офис компании. За два месяца до проведения курсов всем сотрудникам, которых было принято отправить на курсы обучения, присылают информационное письмо с датой и сроками проведения этих курсов.

Сотрудникам филиалов компании, которые приглашены на обучение, покупают билеты на назначенные даты. Так же для них арендуют номера в гостинице. Если сотрудник живет в Петербурге и работает в головном офисе

компании, для него номера не арендуют. Для самих курсов в этом же отеле арендуют конференц-зал на весь срок проведения обучения.

Обучение обычно занимает 3 рабочих дня. Начало обучения в 9-00, окончание в 18-00 с перерывом на обед с 13-00 до 14-00. Для проведения этих курсов компания заключает договор с аккредитованной компанией предоставляющей услуги повышения квалификации по той или иной профессии.

Организаторами составляется перечень тем курсов, которые обязательно касаются области деятельности менеджеров и вопросов информационной безопасности и защиты информации. Тематический план курсов представлен на рисунке 7.

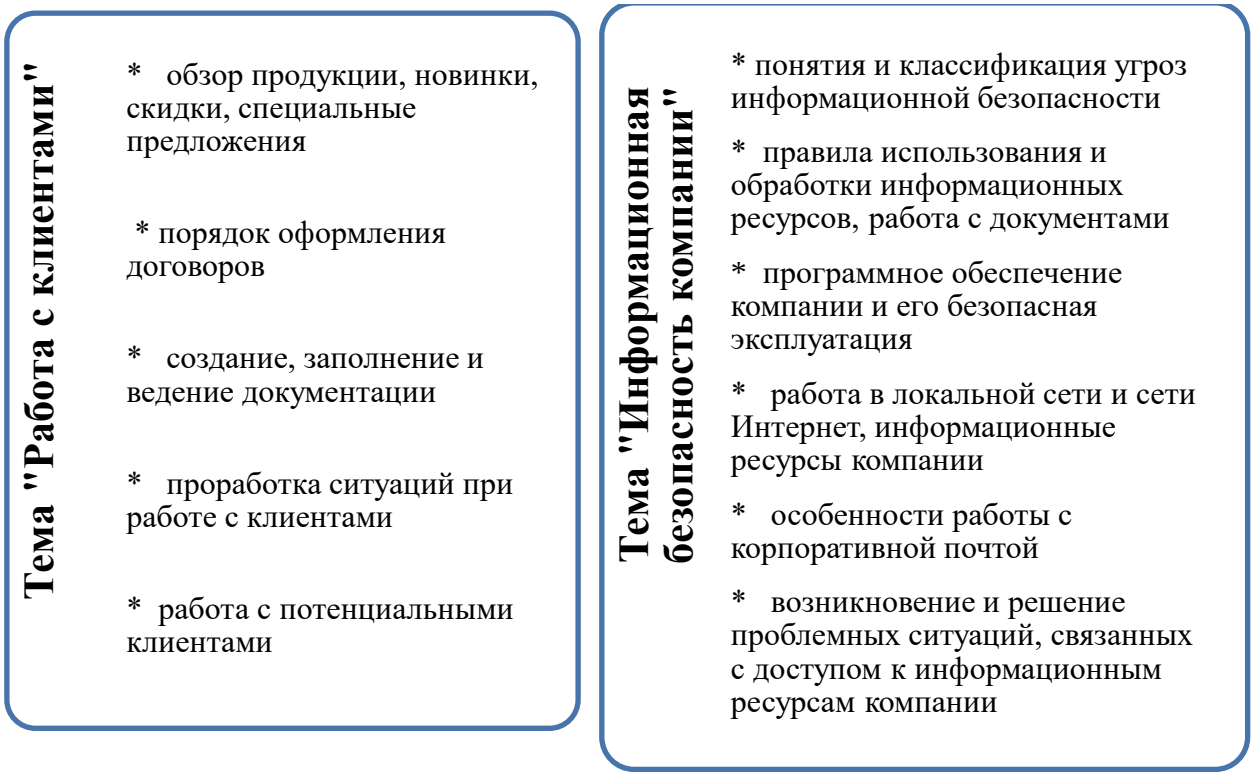

Рисунок 7 — Тематический план курсов дополнительной подготовки

Регламент курсов дополнительной подготовки представлен на рисунке 8.

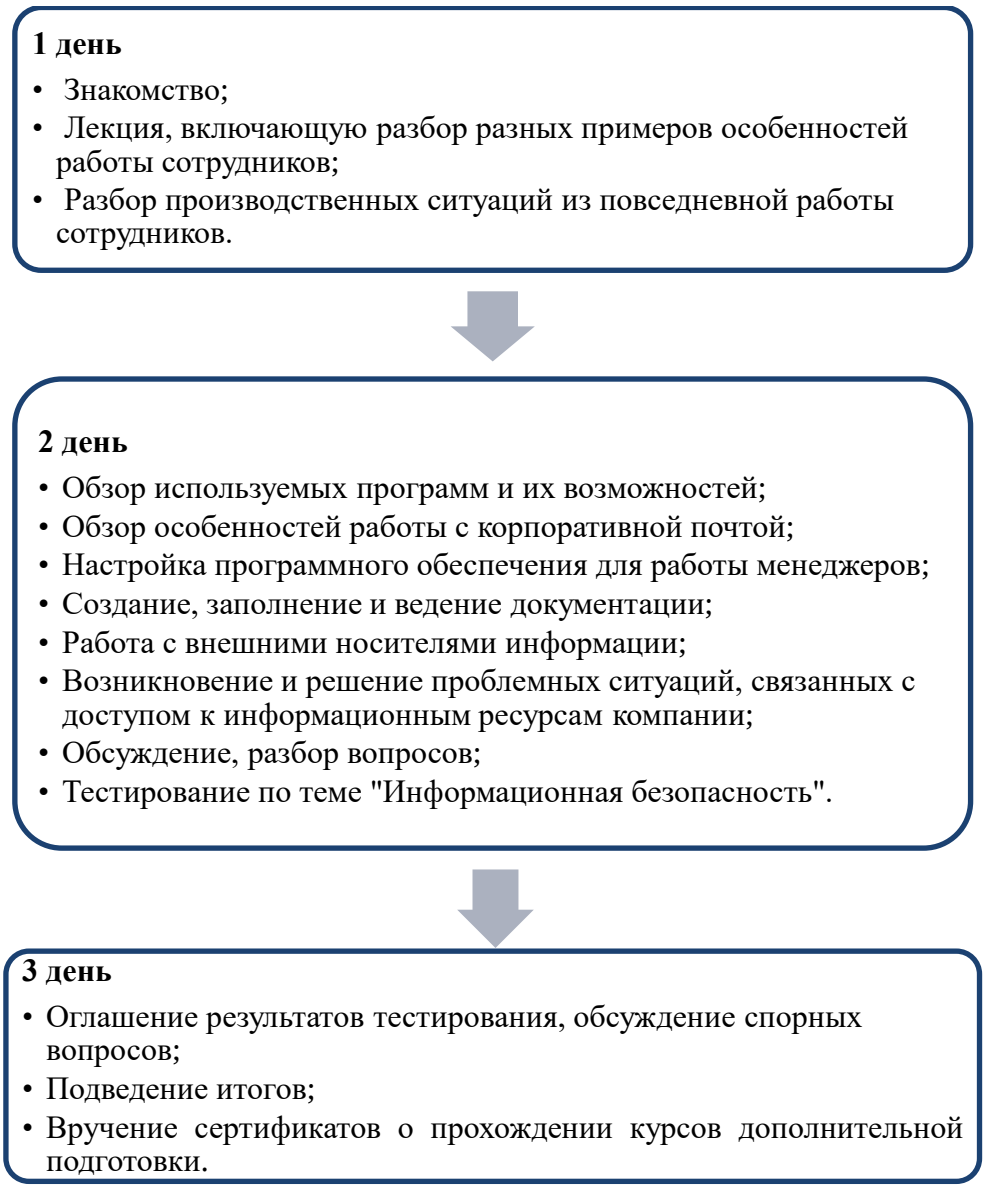

Рисунок 8 — Регламент курсов дополнительной подготовки

1 день. Сбор сотрудников в 9-00 в конференц-зале. Преподаватель со всеми знакомится, узнает о каждом сотруднике информацию о его должности в компании. На основе этой информации в процессе обучения преподаватель старается давать сотруднику именно ту информацию, которая нужна именно ему. Например, менеджеры по продажам и менеджеры по закупкам проходят обучение вместе, но получают информацию и задания, которые более направленны для их профессии. Некоторую универсальную информацию дают менеджерам в равной степени.

После окончания беседы с каждым сотрудником преподаватель начинает лекцию, включающую разбор разных примеров особенностей работы

сотрудников по их направлению (включая и вопросы информационной безопасности).

После обеда начинается разбор производственных ситуаций из повседневной работы сотрудников. Преподаватель помогает разобрать как в той или иной ситуации можно было поступить. Так же эти ситуации проводятся в формате сценки, где сотрудник ставит себя в той же ситуации на свое место, а преподаватель — на место клиента. Ситуацию разбирают, если необходимо сотрудник и преподаватель меняются ролями. По окончанию первого дня в 18-00 преподаватель дает сотрудникам некоторую литературу для самостоятельной подготовки ко второму дню.

2 день. Обучение начинается так же в 9-00 в конференц-зале. Ознакомление с информацией в виде презентации на тему «Информационная безопасность и защита информации».

Далее представлен перечень рассматриваемых вопросов, который может изменяться в соответствии с их актуальностью:

- перечень используемых программ и обзор их возможностей;
- особенности работы с корпоративной почтой;
- настройка программного обеспечения для работы менеджеров;
- создание, заполнение и ведение документации;
- работа с внешними носителями информации;
- возникновение и решение проблемных ситуаций, связанных с доступом к информационным ресурсам компании и др.

Во второй половине дня сотрудники проходят тестирование, в которое включены вопросы по рассмотренным темам.

3 день. В первой половине дня преподаватель дает сотрудникам возможность разбора ситуаций, которые остались не рассмотренными или не до конца понятыми. Преподаватель консультирует сотрудников и отвечает на их вопросы, происходит обсуждение спорных вопросов.

По итогам окончания финального дня преподаватель вручает всем сотрудникам сертификаты о прохождении курсов дополнительной подготовки

и дает им рекомендации, в чем их сильная сторона, а где им необходимо самостоятельно подтянуть знания.

В течение всех 3-х дней обучения присутствует учредитель компании, который так же оценивает действия сотрудников и прислушивается к комментариям преподавателя о профессионализме сотрудников. Присутствие учредителя на этих курсах оказывает дополнительный стресс на процесс обучения.

Так же зачастую на эти курсы обучения приглашают сотрудников, которые работают в компании по много лет. Их основной задачей является помощь в процессе обучения новеньким, они делятся своим опытом.

2.3 Структура электронного пособия

Структура электронного пособия состоит из 5 разделов (рисунок 9):

1. О компании.
2. Общая информация по информационной безопасности.
3. Правила информационной безопасности для менеджеров компании.
4. Программное обеспечение (для менеджеров).
5. Глоссарий.

Информация в электронном пособии разбита на логические темы, чтобы удобнее было с ним работать. В любой момент с помощью гиперссылок можно перемещаться по разделам пособия. Разделы 3, 4 и 5 содержат подразделы. При запуске пособия открывается окно, состоящее из 2 частей: слева будет отображаться оглавление, справа — содержание выбранного пункта. При первом запуске в левой части окна отображается логотип компании, являющийся гиперссылкой, открывающей оглавление пособия, а в правой части — титульная страница (рисунок 10).

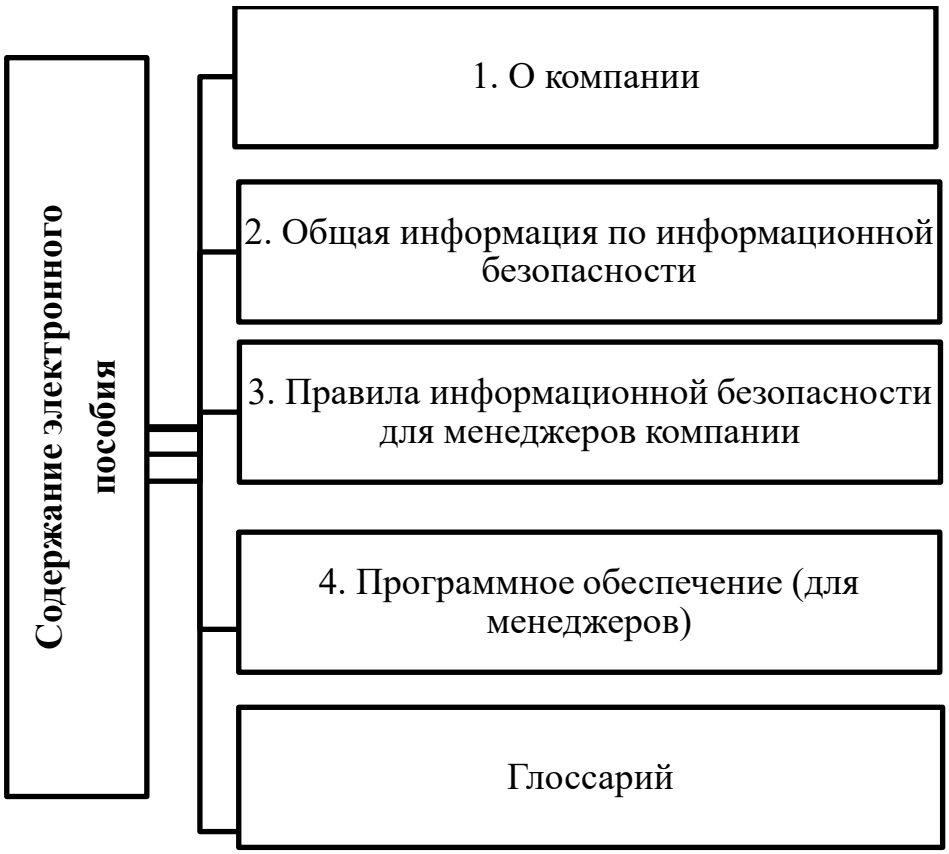

Рисунок 9 — Основные разделы электронного пособия

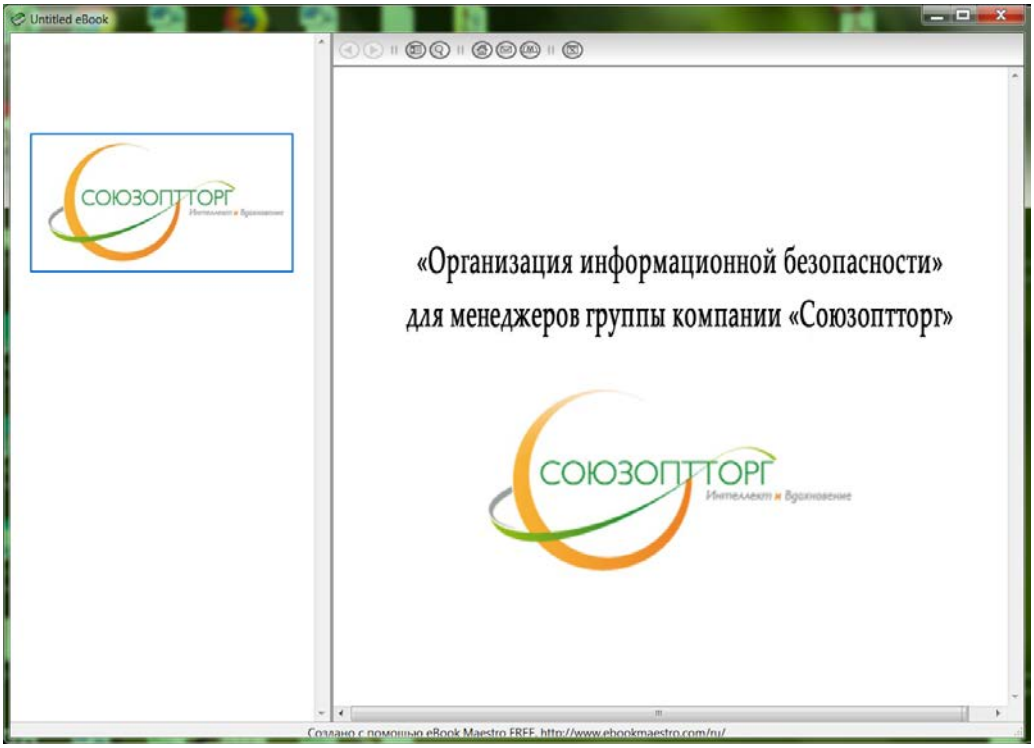

Рисунок 10 — Первый запуск пособия

Окно по умолчанию занимает весь экран, можно его изменять для более удобной работы. При необходимости можно свернуть левую часть, в ко-

торой отображается оглавление, и просматривать только информацию выбранного раздела (рисунок 11).

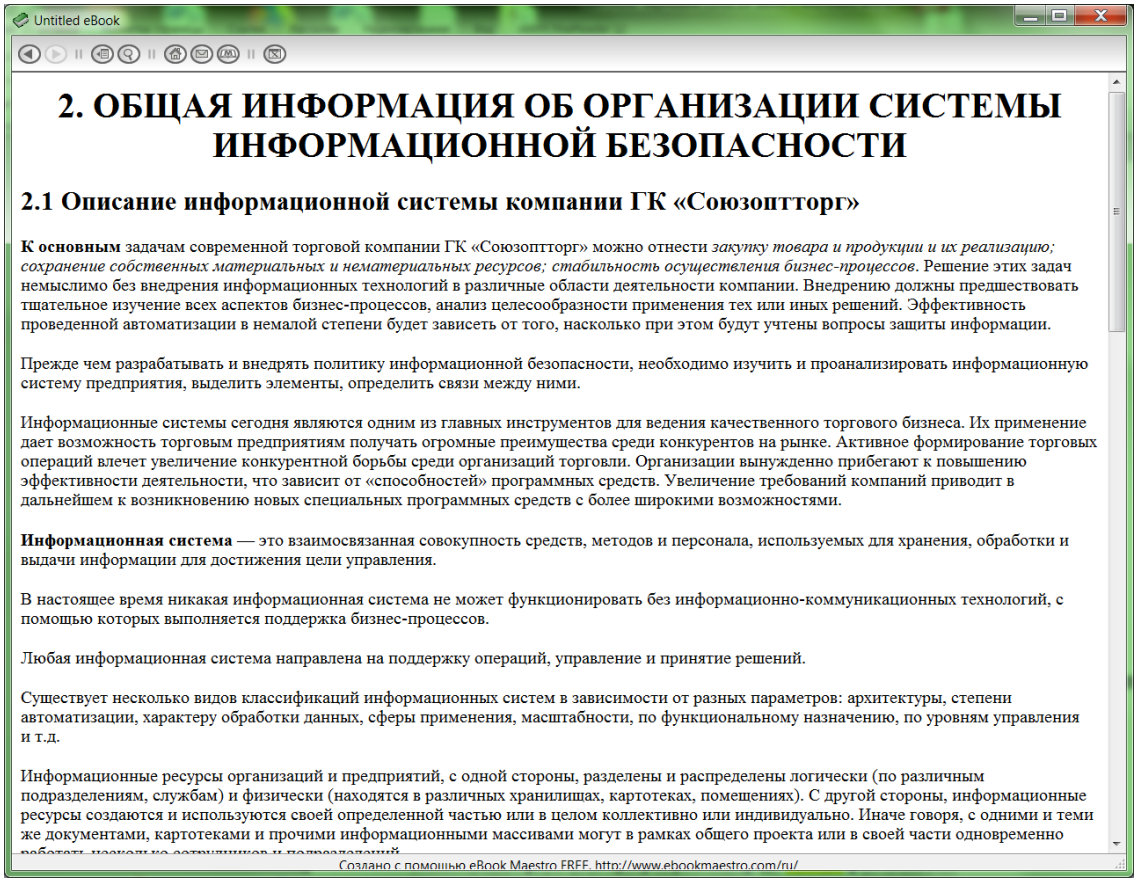

Рисунок 11 — Просмотр информации выбранного раздела при свернутом оглавлении

2.4 Описание электронного пособия

На рисунке 12 представлено полное содержание электронного пособия. Оно отражает основные задачи информационной безопасности, которые требуется освоить менеджерами компании, а именно: производственные цели и задачи, которые реализует компания; общая информация по информационной безопасности, которая раскрывает основные понятия, способы и методы защиты данных; реализуемые для менеджеров компании правила информационной безопасности; используемое менеджерами компании программное обеспечение; глоссарий основных терминов. Внутри разделов информация в электронном пособии разбита на логические темы, для удобства работы с ним.

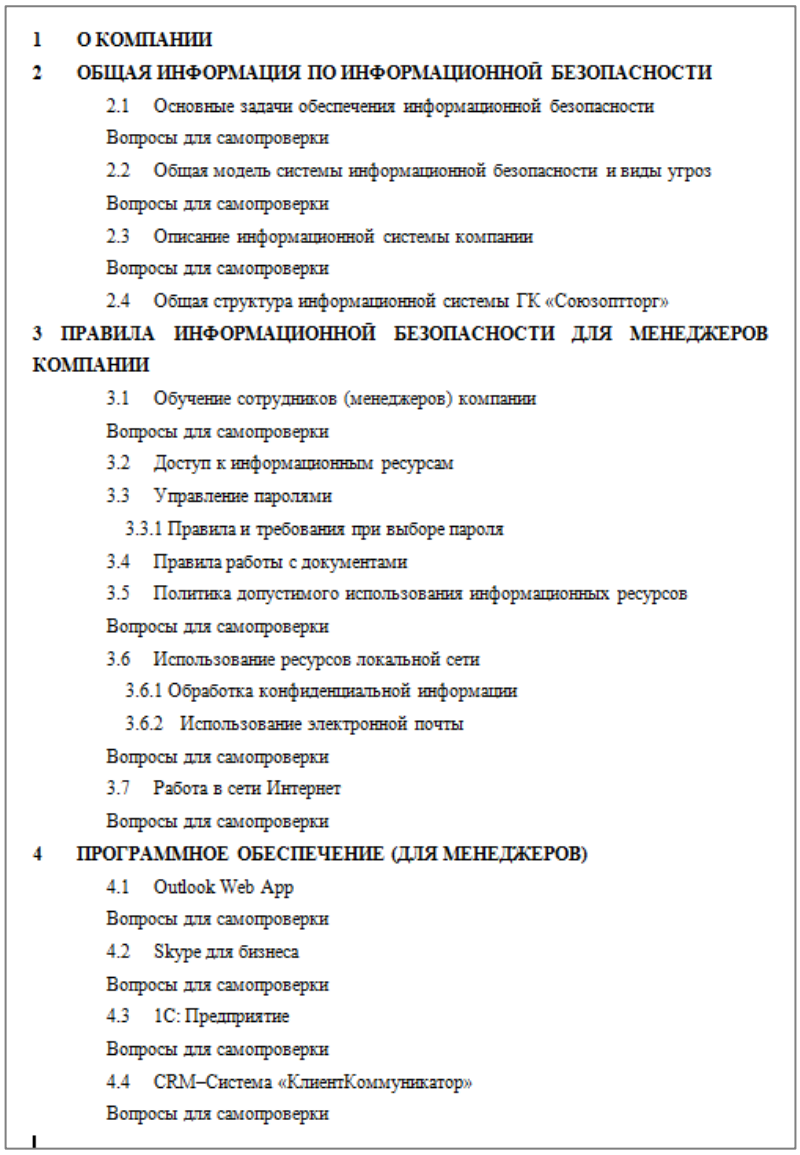

Рисунок 12 — Полное содержание электронного пособия

В разделе «О компании» предоставлена общая информация о группе компаний «Союзоптторг». Это один из ведущих дистрибьюторов пищевых ингредиентов в России и странах СНГ. Компания предлагает более 2000 наименований продуктов и добавок от ведущих мировых производителей. Предлагаемые основные группы ингредиентов: улучшающие внешний вид, изменяющие структуру и физико-химические свойства, влияющие на вкус и аромат, замедляющие микробную и окислительную порчу пищевых продуктов. Для ознакомления с более подробной информацией и деятельности компании представлена ссылка на его сайт.

Фрагмент раздела представлен на рисунке 13.

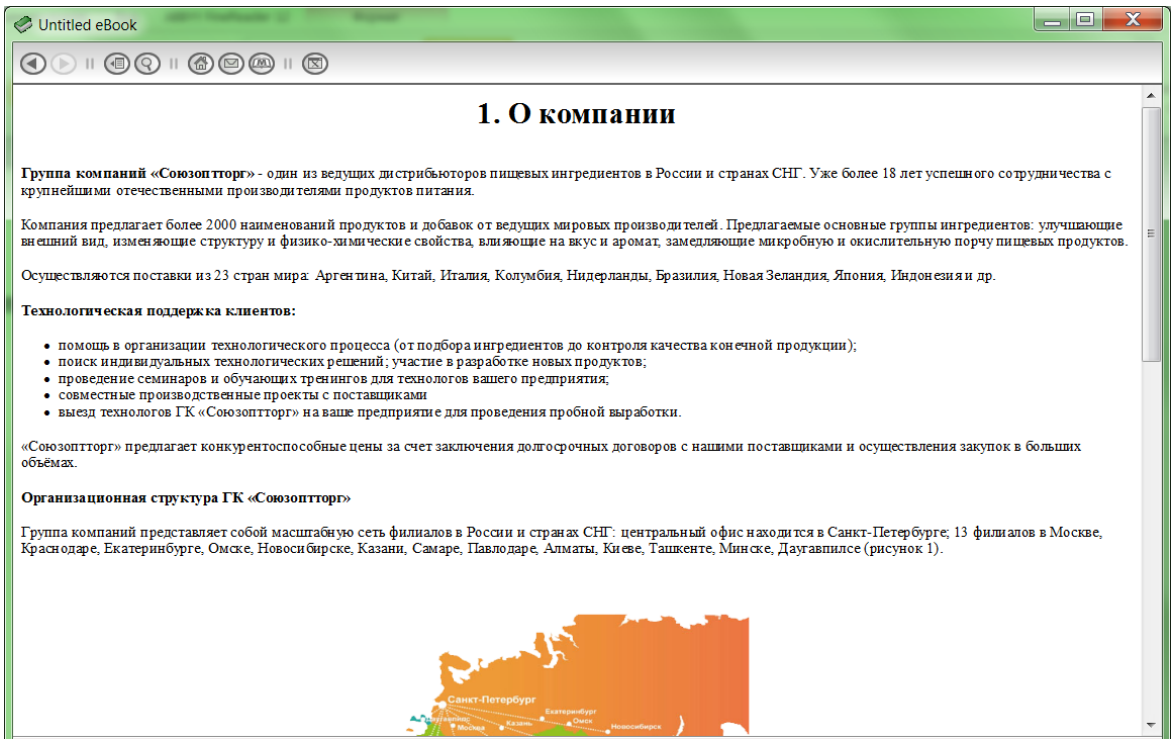

Рисунок 13 — Фрагмент раздела «О компании»

Раздел «Общая информация по информационной безопасности» состоит из 4-х подразделов:

- основные задачи обеспечения информационной безопасности;
- общая модель системы информационной безопасности и виды угроз;
- описание информационной системы компании;
- общая структура информационной системы ГК «Союзоптторг». Фрагмент раздела представлен на рисунке 14.

Раздел «Правила информационной безопасности для менеджеров компании» состоит из 7-и подразделов (рисунок 15):

- обучение сотрудников (менеджеров) компании;
- доступ к информационным ресурсам;
- управление паролями;
- правила работы с документами;
- правила допустимого использования информационных ресурсов;
- использование ресурсов локальной сети;
- работа в сети Интернет.

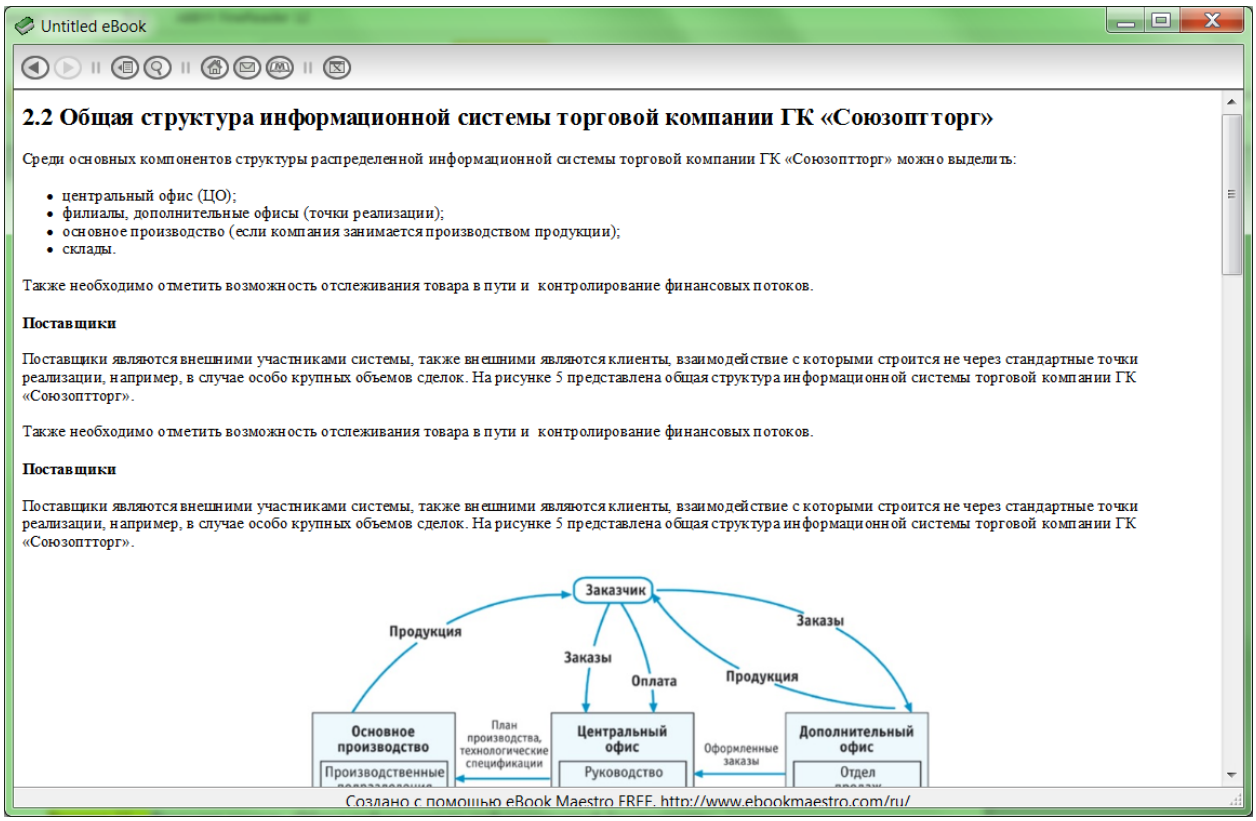

Рисунок 14 — Фрагмент раздела «Общая информация по информационной безопасности»

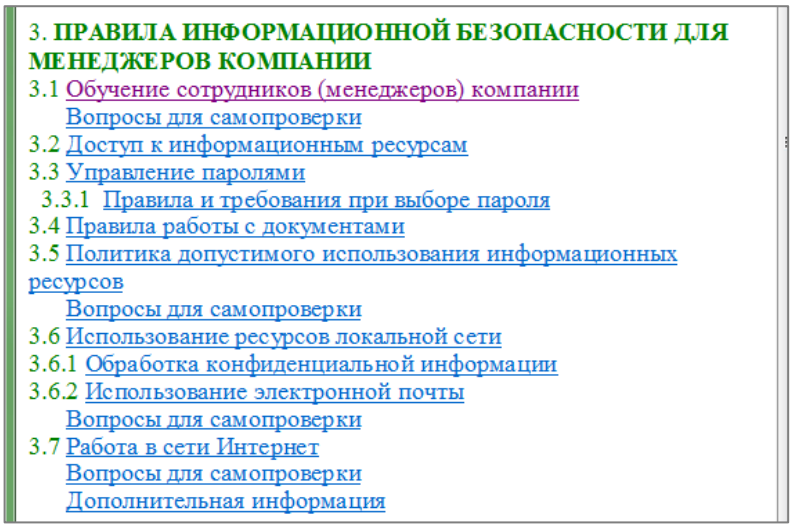

Рисунок 15 — Оглавление раздела «Правила информационной безопасности для менеджеров компании»

В этом разделе рассматривается наиболее важная информация, касающаяся вопросов информационной безопасности и защиты информации при работе в информационной системе компании. Фрагмент раздела представлен на рисунке 16.

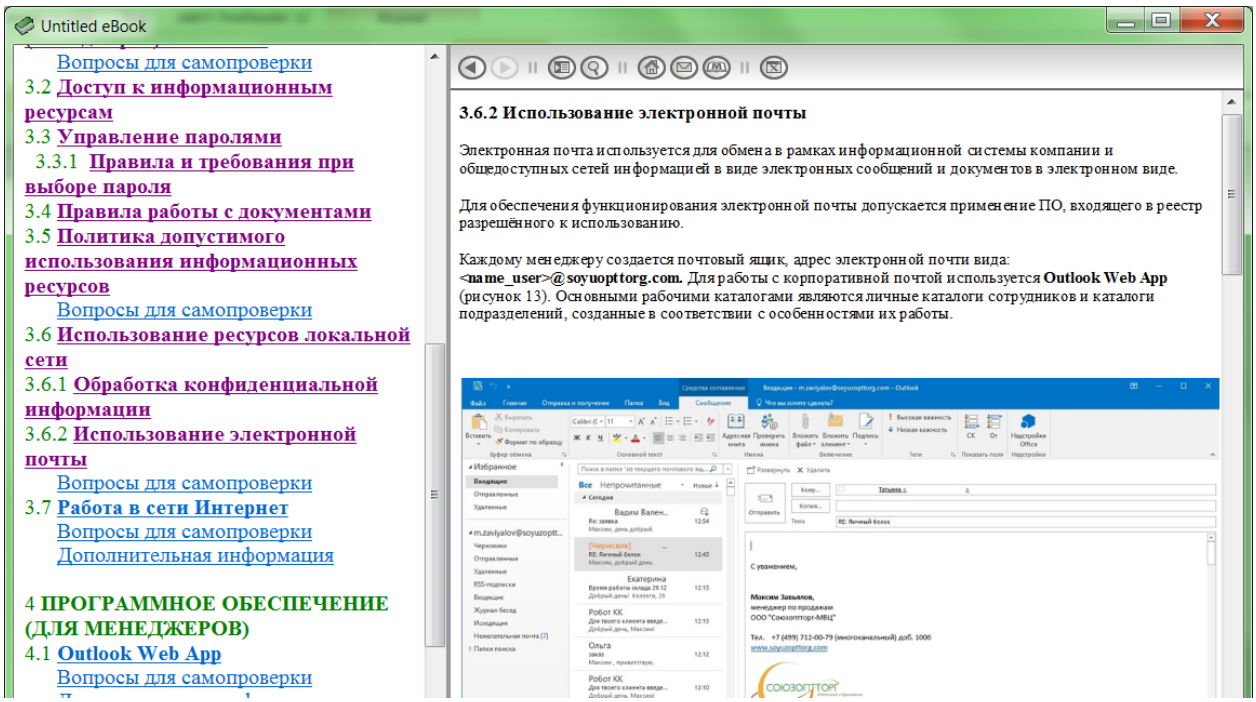

Рисунок 16 — Фрагмент раздела «Правила информационной безопасности для менеджеров компании»

В конце некоторых подразделов составлены вопросы для самопроверки для закрепления рассмотренного материала (рисунок 17).

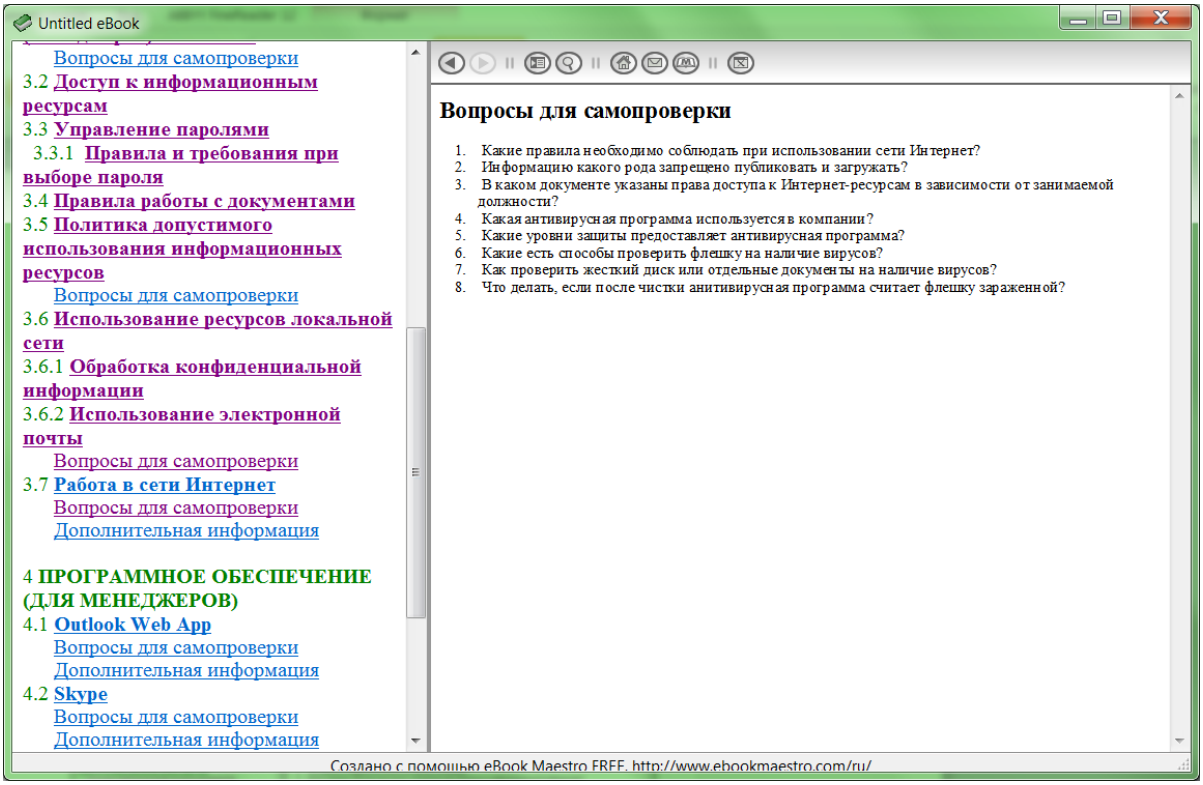

Рисунок 17 — Вопросы для самопроверки одного из подразделов

В разделе «Программное обеспечение (для менеджеров)» рассмотрены основные программы, с которыми постоянно работают менеджеры:

- Outlook Web App;
- Skype;
- 1С: Предприятие;
- CRM-Система «Клиент-Коммуникатор».

Оглавление этого раздела представлено на рисунке 18.

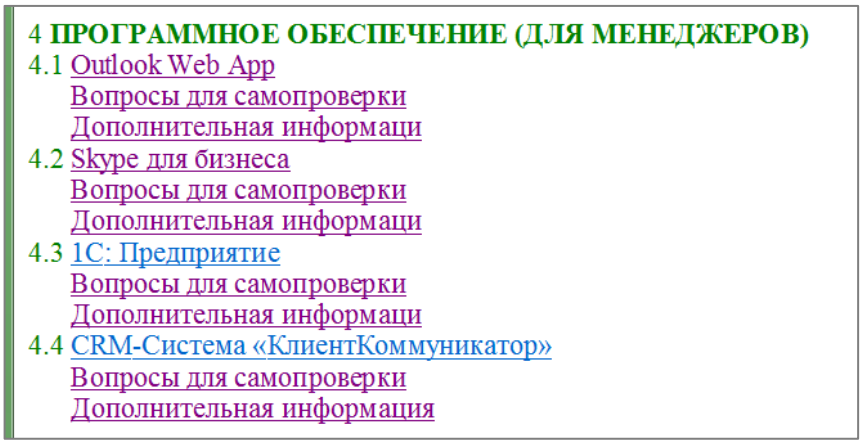

Рисунок 18 — Оглавление раздела «Программное обеспечение (для менеджеров)»

Outlook Web App используется как корпоративная почта, предоставляет удобные сервисы, такие как Почта, Задачи, Календарь, Календарь.

Skype — коммуникационная программа-клиент, позволяющая пользователям общаться друг с другом в реальном времени, используя различные виды коммуникаций: мгновенные сообщения, видео- и голосовую связь, общий доступ к рабочему столу, конференции, передачу файлов.

1С:Предприятие — программный продукт компании «1С», предназначенный для автоматизации деятельности на предприятии.

Система программ «1С:Предприятие 8.х» включает в себя саму платформу и программные продукты, разработанные на ее основе для ведения учета, например «1С:Бухгалтерия 8». На одной платформе можно автоматизировать деятельность подразделений компании, разных компаний и направлений бизнеса, докупая соответствующие конфигурации программ и интегрируя их в единое информационное пространство.

«Клиент—Коммуникатор» («КлиК») представляет собой мощную CRM/ERP систему, которая построена по клиент-серверной архитектуре. В качестве СУБД используется MS SQL Server.

Программный комплекс Клиент-Коммуникатор — это специально разработанная платформа для визуального проектирования систем управления предприятием. Продуманная отлаженная архитектура и прикладные инструменты, позволяют максимально полно и быстро реализовывать типовые и специфические задачи автоматизации предприятий, работающих в различных отраслевых сегментах.

Каждая из рассмотренных программ предоставляет менеджеру информацию, связанную с его областью деятельности, например, контакты коллег или партнеров. Фрагмент этого раздела представлен на рисунке 19.

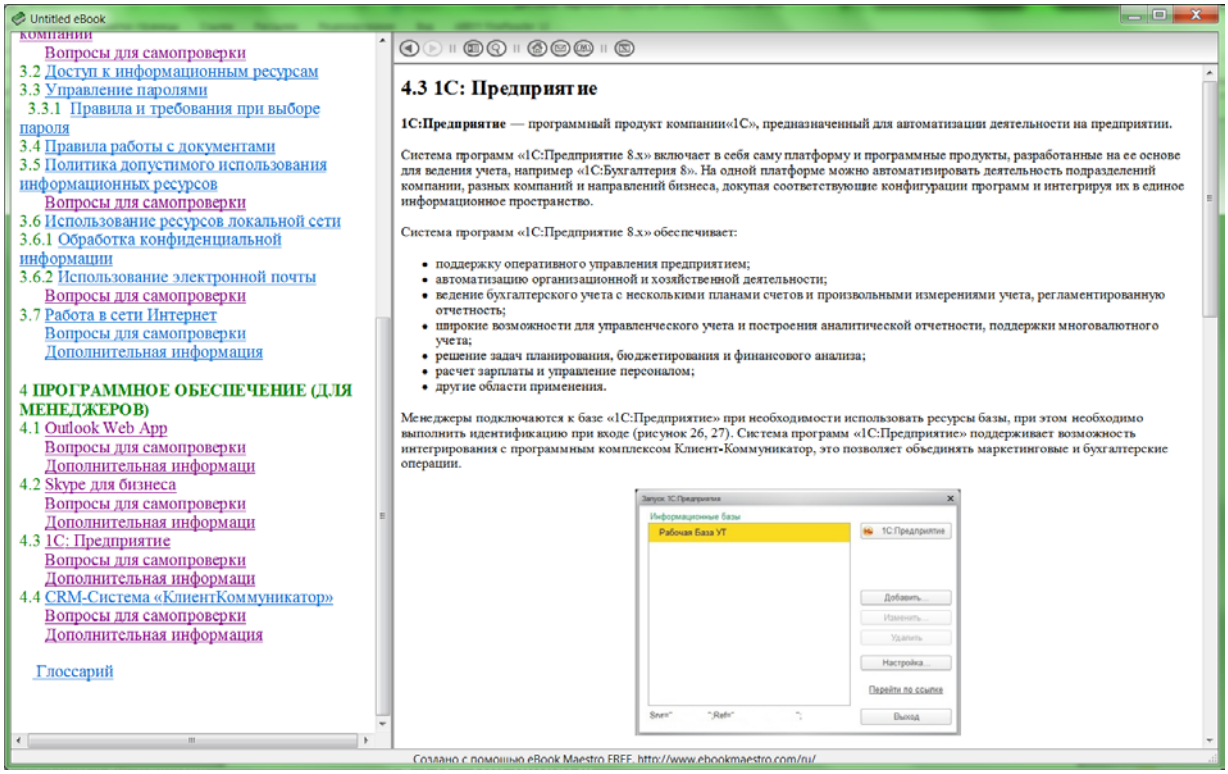

Рисунок 19 — Фрагмент раздела «Программное обеспечение (для менеджеров)»

В конце подразделов также имеются вопросы для самопроверки, касающиеся рассмотренной информации. Также предлагается ознакомиться с дополнительной информацией, которая располагается в одноименном подразделе. Гиперссылки в виде кнопок позволяют перейти на внешний сайт и

ознакомиться с информацией подробнее, сайт откроется в браузере. Пример подраздела с дополнительной информацией представлен на рисунке 20.

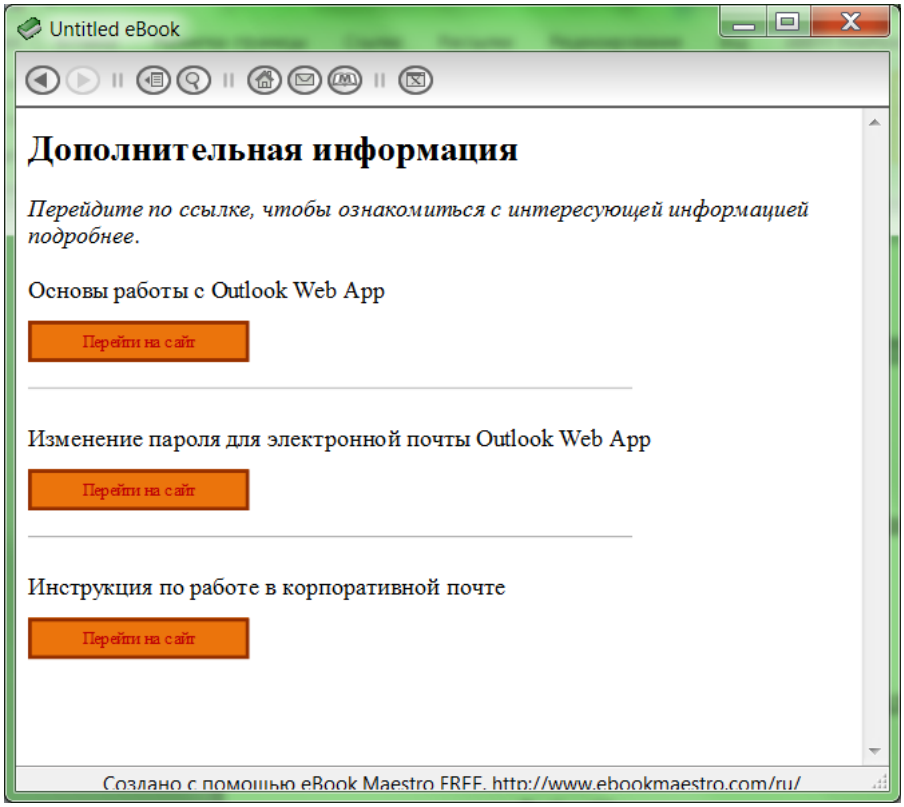

Рисунок 20 — Подраздел с дополнительной информацией

Последним пунктом в оглавлении пособия указан Глоссарий. В этом разделе собраны наиболее важные термины по информационной безопасности. Фрагмент раздела «Глоссарий» представлен на рисунке 21.

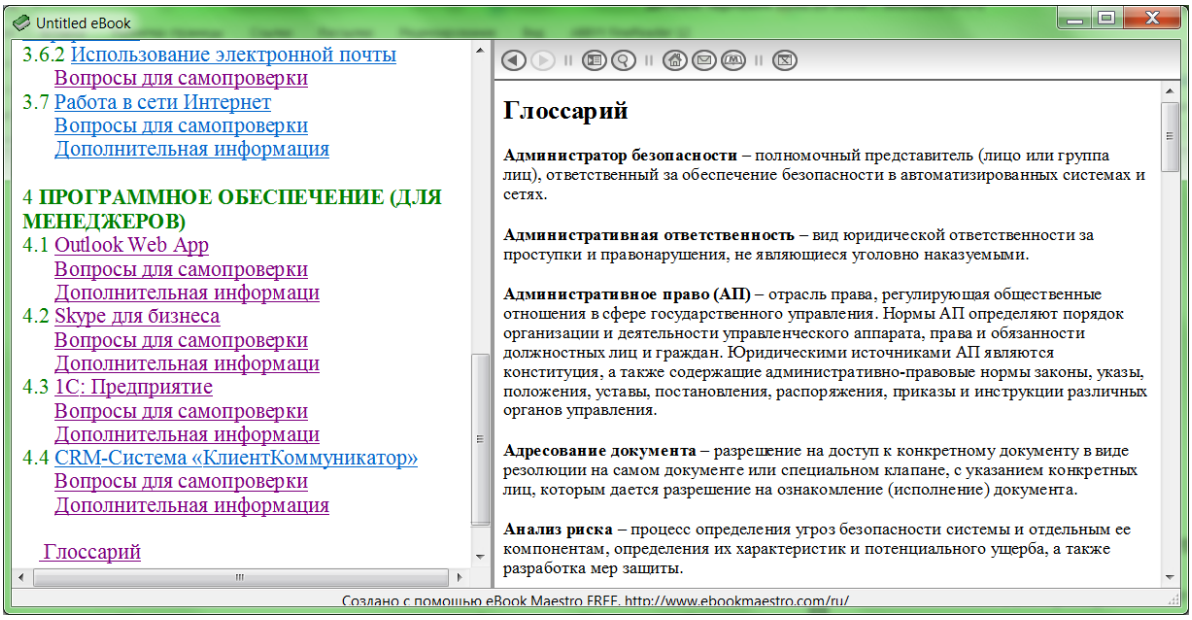

Рисунок 21 — Фрагмент раздела «Глоссарий»

2.5 Средства реализации электронного пособия

Для наполнения, компоновки и форматирования содержимого инструкции использовался текстовый процессор MS Word. Для электронной версии материал был преобразован в формат .html. Каждый раздел хранится в отдельном файле формата .html (рисунок 22).

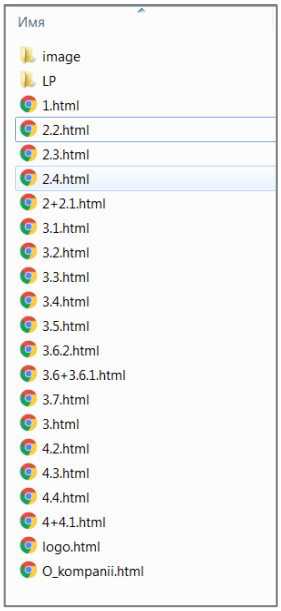

Рисунок 22 — Структура файлов и папок для электронного пособия

Для преобразования и редактирования текстовых файлов в формат .html использовался редактор Tiny (рисунок 23).

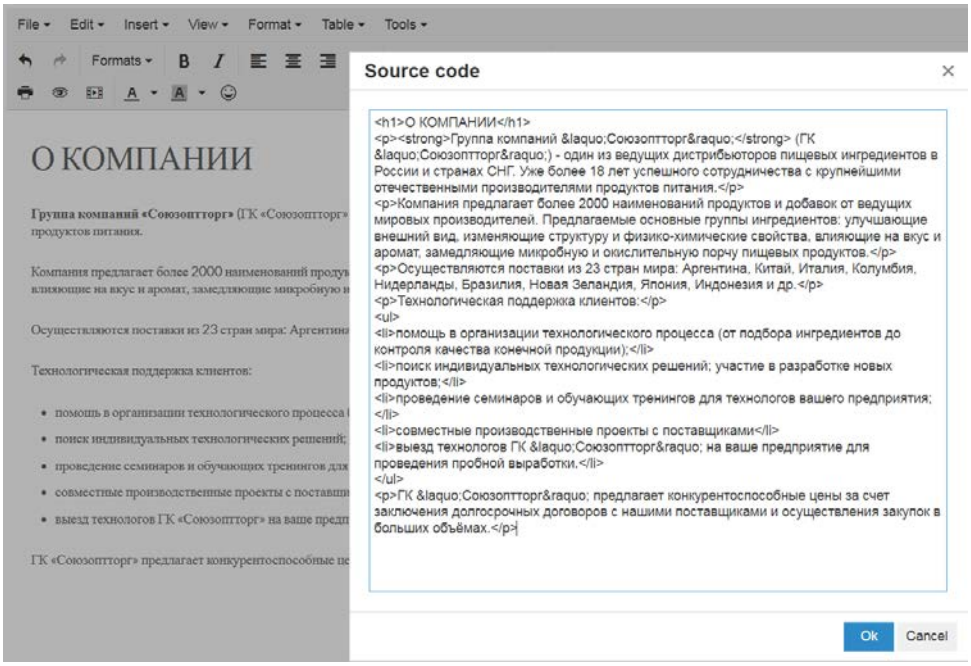

Рисунок 23 — Редактор Tiny

Для сборки файлов в электронное пособие использовалась бесплатная программа eBook Maestro. **eBook Maestro** — это программа для создания информационных продуктов (например, электронные книги, презентации, журналы, альбомы, галереи, руководства, офлайн web-сайты, отчеты, тренировочные курсы, тесты, опросники и т.д.)

Электронные книги, создаваемые с помощью этой программы, могут содержать и открывать любые типы файлов: HTML-страницы, графические файлы, Flash файлы, Java скрипты, VB скрипты, каскадные таблицы стилей (CSS), звуковые файлы, видео файлы, и т.д.

Компилятор eBook Maestro превращает HTML-страницы (веб-сайты) в электронные книги в формате исполняемых приложений. Такие книги напоминают веб-браузеры, которые позволяют перемещаться по скомпилированному веб-сайту, будто они подключены к Интернету.

После компиляции с помощью eBook Maestro веб-сайт превращается в самостоятельное приложение, называемое *электронной книгой* или *электронной публикацией*. Получившийся исполняемый файл можно посылать пользователям. Работать с файлами можно без каких-либо дополнительных программ для просмотра и без необходимости в исходных HTML-страницах веб-сайта [20].

При создании, можно настроить следующие параметры:

- общие (название книги, контактные данные автора, адрес сайта автора).
- файлы (местоположение файлов, местоположение итогового файла).
- интерфейс (настройка элементов интерфейса).
- инфо (справочная информация о программе EBook Maestro).

После всех настроек можно выполнить компиляцию, а можно сохранить все настройки, чтобы в случае внесения изменений не пришлось всё настраивать заново. Параметры сохраняются в файле с расширением .ebm.

При дальнейшем изменении или добавлении разделов, необходимо перекомпилировать файл.

При настройке интерфейса итогового файла можно указать наличие элемента интерфейса, а также его размеры минимальные и максимальные в случае изменения размеров окна (рисунок 24).

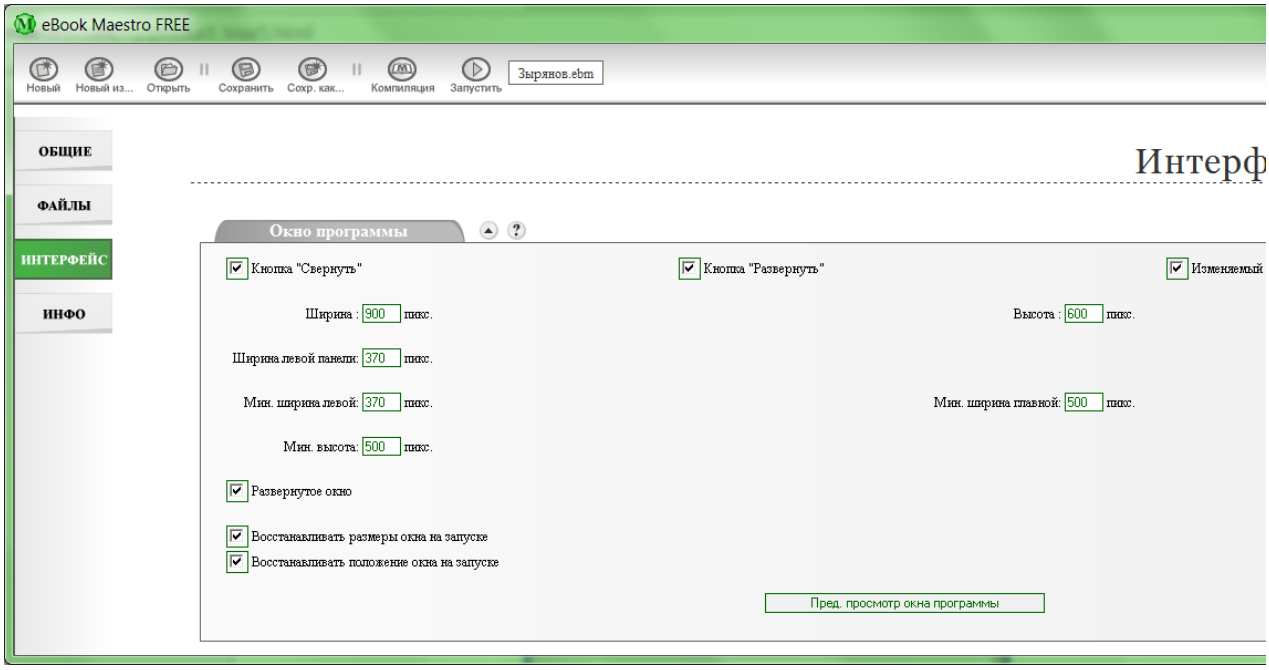

Рисунок 24 — Настройки интерфейса

В итоге файл представляет собой формат exe, который можно запустить на любой системе (рисунок 25).

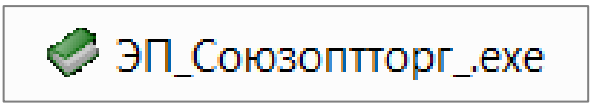

Рисунок 25 — Пиктограмма файла пособия

ЗАКЛЮЧЕНИЕ

В соответствии с задачами выпускной квалификационной работы были рассмотрены теоретические основы обеспечения информационной безопасности в торговле, а именно проанализировано современное состояние информационной безопасности в торговле, рассмотрены современные угрозы информационной безопасности в торговых компаниях. В результате сделан вывод о росте требований к информационным технологиям, к информационной безопасности в организациях торговли.

Следующий этап работы — анализ литературы и интернет источников по темам «Информационная безопасность», «Защита информации», необходимый для разработки учебного пособия, что позволило понять теоретическую сторону исследуемой темы и систематизировать материал. Также проведен анализ существующих электронных пособий для менеджеров торговых компаний и сделан вывод о том, что разработка электронного пособия по организации информационной безопасности для менеджеров торговой компании, актуальна.

В рамках решения задачи по разработке электронного пособия были рассмотрены: организационная структура компании, информационные ресурсы и программное обеспечение, реализованное в виде распределенной информационной системы компании, выявлены основные задачи информационной безопасности, эффективное решение которых повлияет на повышение безопасной работы менеджеров по торговле и, соответственно, повысит качество их профессиональной деятельности. В соответствии с этими задачами разработана структура и содержание пособия для самоподготовки менеджеров компании при прохождении тестирования на курсах дополнительной подготовки. Для электронной версии материал был преобразован в формат .html. Таким образом, поставленные задачи были решены, цель выпускной квалификационной работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аудит информационной безопасности [Электронный ресурс]. — Режим доступа: https://www.pentestit.ru/audit/ (дата обращения: 12.11.2018).

2. Баранова Е. К. Информационная безопасность и защита информации [Текст]: учебное пособие / Е. К. Баранова, А. В. Бабаш. — 3-е изд., перераб. и доп. — Москва: ИНФРА-М, 2017. — 322 с.

3. Баранова Е. К. Информационная безопасность и защита информации [Электронный ресурс]. — Режим доступа: http://znanium.com/bookread2.php?book=763644&spec=1 (дата обращения: 20.11.2018).

4. Беляев В. И. Безопасность в распределенных системах [Электронный ресурс]. — Режим доступа: https://www.osp.ru/os/1995/03/178633/ (дата обращения: 12.12.2018).

5. Бондаренко С. Идентификация, аутентификация, авторизация — в чем разница? [Электронный ресурс]. — Режим доступа: http://it-uroki.ru/uroki/bezopasnost/identifikaciya-autentifikaciya-avtorizaciya.html (дата обращения: 20.11.2018).

6. Гатчин Ю. А. Основы информационной безопасности [Электронный ресурс]. — Режим доступа: http://www.ict.edu.ru/ft/006193/itmo378.pdf (дата обращения: 12.12.2018).

7. Гатчин Ю. А. Основы информационной безопасности: Учеб. пособие [Текст] / Ю. А. Гатчин, Е. В. Климова. — Санкт-Петербург: СПбГУ ИТМО, 2009. — 84 с.

8. Грушо А. Защита распределенных компьютерных систем [Электронный ресурс]. — Режим доступа: http://sec4all.net/comprasp-prot.html (дата обращения: 20.11.2018).

9. Инструкция по работе в корпоративной почте [Электронный ресурс]. — Режим доступа: https://www.vyatsu.ru/uploads/file/1603/

instrukciya_po_rabote_s_korporativnoy_pochtoi_dlya_sotrudnikov_vyatggu.pdf (дата обращения: 25.11.2018).

10. Информационная безопасность предприятия: ключевые угрозы и средства защиты [Электронный ресурс]. — Режим доступа: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html (дата обращения: 20.11.2018).

11. Информационно-технологическое сопровождение пользователей 1С: Предприятие [Электронный ресурс]. — Режим доступа: https://its.1c.ru/ (дата обращения: 20.11.2018).

12. Как ограничить доступ к ресурсам с помощью антивируса Касперского [Электронный ресурс]. — Режим доступа: https://www.kaspersky.ru/blog/sovet-nedeli-kak-ogranichit-dostup-dlya-rebenka-k-opredelennym-sajtam/970/ (дата обращения: 12.01.2019).

13. КлиК. Управление. Руководство пользователя (полная инструкция по работе) [Электронный ресурс]. — Режим доступа: http://sysclick.ru/uploads/images/documentation/Manual_Base.pdf (дата обращения: 20.01.2019).

14. Комплект типовых документов по информационной безопасности [Электронный ресурс]. — Режим доступа: http://www.globaltrust.ru/ru/produkty/komplekty-dokumentov-po-informacionnoi-bezopasnosti/tipovye-organizacionno-rasporyaditelnye-dokumenty-po-informacionnoi-bezopasnosti (дата обращения: 12.01.2019).

15. Медведев К. Информационная безопасность: что может сделать HR [Электронный ресурс]. — Режим доступа: https://www.rabota.ru/articles/hr/hr-security-142 (дата обращения: 12.12.2018).

16. Модели информационной безопасности в работе Windows VPS [Электронный ресурс]. — Режим доступа: https://habr.com/company/vps_house/blog/347088/ (дата обращения: 20.12.2018).

17. Настройка автоматической проверки флешки на вирусы [Электронный ресурс]. — Режим доступа: https://www.kaspersky.ru/blog/sovet-nedeli-

avtomaticheskaya-proverka-fleshek-pri-podklyuchenii-k-kompyuteru/1189/ (дата обращения: 20.11.2018).

18. Обеспечение информационной безопасности организации системах [Электронный ресурс]. — Режим доступа: http://www.iccwbo.ru/-blog/2016/-obespechenie-informatsionnoy-bezopasnosti/ (дата обращения: 20.11.2018).

19. Обучающие материалы по возможностям антивируса Касперского [Электронный ресурс]. — Режим доступа: https://support.kaspersky.ru/learning/courses/kl_102.10 (дата обращения: 12.01.2019).

20. Описание программы eBook Maestro [Электронный ресурс]. — Режим доступа: http://www.ebookmaestro.com/ru/ (дата обращения: 25.11.2018).

21. Основные термины и определения из области информационной безопасности [Электронный ресурс]. — Режим доступа: https://studfiles.net/preview/5823054/page:3/ (дата обращения: 20.11.2018).

22. Основы работы с Outlook Web App [Электронный ресурс]. — Режим доступа: https://support.office.com/ru-ru/article/%D0%9D%D0%B0%D1%87%D0%B0%D0%BB%D0%BE-%D1%80%D0%B0%D0%B1%D0%BE%D1-%82%D1%8B%D1%81-outlook-d59155ff-af58-4f1f-a892-0e8bde098e43?ui=ru-RU&rs=ru-RU&ad=RU#ID0EAABAAA=Set_up_accounts (дата обращения: 12.12.2018).

23. Розничная торговая сеть [Электронный ресурс]. — Режим доступа: https://znaytovar.ru/s/Roznichnaya-torgovaya-set.html (дата обращения: 12.11.2018).

24. Розничные торговые сети [Электронный ресурс]. — Режим доступа: http://www.grandars.ru/college/biznes/torgovye-seti.html (дата обращения: 20.11.2018).

25. Руководство пользователя по работе с модулем «СКАНЕР OUTLOOK» в программе «Клиент-Коммуникатор» [Электронный ресурс]. — Режим доступа: http://sysclick.ru/uploads/images/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D1%8F/Manual_OutlookScanner.pdf (дата обращения: 19.01.2019).

26. Руководство пользователя ЭДО без электронной подписи для участников 1С: Бизнес-сеть [Электронный ресурс]. — Режим доступа: https://portal.1c.ru/download/public/instruction/guide_1c_BN_account.pdf (дата обращения: 22.12.2018).

27. Русинов С. Обеспечение информационной безопасности предприятий торговли, торговых сетей и их инфраструктуры [Электронный ресурс]. — Режим доступа: http://itsec.ru/articles2/Inf_security/infosec-torg (дата обращения: 20.11.2018).

28. Система управления бизнесом Руководство пользователя по работе с модулем «Клиент-Коммуникатор» [Электронный ресурс]. — Режим доступа: http://sysclick.ru/uploads/images/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D1%8F/Manager_manual.pdf (дата обращения: 19.01.2019).

29. Теренин А. А. Торговля и безопасность [Электронный ресурс]. — Режим доступа: http://itsec.ru/articles2/focus/torgovlya_i_bezopasnosti (дата обращения: 12.12.2018).

30. Утечки информации в розничных торговых сетях: специфика и методы борьбы [Электронный ресурс]. — Режим доступа: https://securenews.ru/retail_leaks/ (дата обращения: 20.11.2018).

31. Филатова В. О. 1С: Предприятие 8.3. Бухгалтерия предприятия, Управление торговлей, Управление персоналом [Электронный ресурс]. — Режим доступа: http://diplom-college.ru/a/kimb/files/23892/26230/ Filatova_V._1S_Predpriyatie _8.3.pdf (дата обращения: 22.12.2018).

32. Фирсова О. А. Экономическая безопасность предприятия [Электронный ресурс]. — Режим доступа: https://marketing.wikireading.ru/5750 (дата обращения: 22.12.2018).

33. Эрганова Н. Е. Практикум по методике профессионального обучения [Текст]: учебное пособие / Н. Е. Эрганова. — Екатеринбург: Изд-во Рос. гос. проф.-пед.ун-та, 2011. — 89 с.

ПРИЛОЖЕНИЕ

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

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль «Информатика и вычислительная техника»

Профилизация «Информационная безопасность»

УТВЕРЖДАЮ
Заведующий кафедрой
_____ И. А. Суслова
подпись и.о. фамилия

« ___ » _____ 2019 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента (ки) *5* курса группы *ЗИБ-501*
Завьялов Максим Андреевич
фамилия, имя, отчество полностью

1. Тема ***Электронное пособие «Организация информационной безопасности менеджеров торговой компании»***
утверждена распоряжением по институту от «_____» _____ 2018 г. № ___
2. Руководитель ***Телепова Татьяна Петровна***
фамилия, имя, отчество полностью

_____ _____ *Ст. преподаватель* *РГППУ*
ученая степень ученое звание должность место работы

3. Место преддипломной практики *Группа компаний «Союзоптторг»*

4. Исходные данные к ВКР *Русинов С. Обеспечение информационной безопасности предприятий торговли, торговых сетей и их инфраструктуры*
5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов):
1. Теоретические основы обеспечения информационной безопасности в торговле;
2. Анализ задач по организации информационной безопасности менеджеров торговой компании;

3. Разработать структуру электронного пособия и отобрать информацию, необходимую для подготовки менеджеров по продажам к тестированию;

4. Разработать электронный вариант пособия.

6. Перечень демонстрационных материалов *Презентация, выполненная в MSPowerPoint, электронное пособие*

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной квалификационной работе	21.01.2019	20%	подпись
2	Выполнение работ по разрабатываемым вопросам и их изложение в пояснительной записке:		60%	подпись
2.1	Изучить теоретические основы обеспечения информационной безопасности в торговле	27.01.2019	10%	подпись
2.2	Проанализировать задачи по организации информационной безопасности менеджеров торговой компании.	30.01.2019	15%	подпись
2.3	Разработать структуру электронного пособия и отобрать информацию, необходимую для подготовки менеджеров по продажам к тестированию	05.02.2019	20%	подпись
2.4	Разработать электронный вариант пособия.	10.02.2019	15%	подпись
3	Оформление текстовой части ВКР	12.02.2019	5%	подпись
4	Выполнение демонстрационных материалов к ВКР	15.02.2019	5%	подпись
5	Нормоконтроль	15.02.2019	5%	подпись
6	Подготовка доклада к защите в ГЭК	16.01.2019	5%	подпись

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ *Задание получил* _____
подпись дата подпись студента дата

9. Дипломная работа и все материалы проанализированы.

Считаю возможным допустить ***Завьялов М. А.*** к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____
подпись дата

10. Допустить ***Завьялова М. А.*** к защите выпускной квалификационной работы
фамилия и. о. студента

в государственной экзаменационной комиссии (протокол заседания кафедры от «___» _____ 20___г., № _____)

Заведующий кафедрой _____
подпись дата