ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ЭКОНОМИКИ И УПРАВЛЕНИЯ

КАФЕДРА ЭКОНОМИКИ И МОДЕЛИРОВАНИЯ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ

РАЗРАБОТКА ПРОЕКТА ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Выпускная квалификационная работа
обучающегося по специальности
38.05.01 Экономическая безопасность
очной формы обучения,
группы 09001411
Столбовского Максима Леонидовича

Научный руководитель
к.э.н., доцент Кулик А.М.

Рецензент
генеральный
директор Алешкин А.А.

БЕЛГОРОД 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Под информационной безопасностью понимают состояние защищенности информационной среды, обеспечивающее ее формирование и развитие. Управление предприятием не может эффективно проводиться без достаточной оперативной, надеждой, своевременной и достоверной информации. Информация является основой управленческого процесса, и от того, насколько она совершенна, во многом зависит качество управления предприятием. Информационная деятельность требует от него чёткой организации процесса сбора, анализа и обработки информации, причём он должен уметь определять важность или второстепенность поступающей информации. Опытный менеджер также должен иметь упорядочивать коммуникации и обмен информацией в рамках предприятия и фирмы.

В условиях постоянного роста количества известных и появления новых видов информационных угроз перед крупными предприятиями всё чаще встаёт задача обеспечения надёжной защиты корпоративных сетей от вредоносных программ и сетевых атак.

Работа с информацией в современных условиях отличается не только массивом и многообразием ресурсов, постоянным обновлением технологий ее обработки, повышенным вниманием и контролем над персоналом, но и грамотным уровнем управления фирмой. Известно, что процесс массового внедрения компьютерной техники и информационных технологий наряду с прогрессивным началом неизбежно создает и дополнительные проблемы. Они связаны с реальными угрозами безопасности предприятий, с потерей стратегически важной информации, а вместе с этим и утратой управляемости компании.

В целях сокращения побочных явлений повсеместного использования новых информационных технологий руководство организаций определяет стратегию своей деятельности в информационной сфере. Стержневым началом такой стратегии должна быть информационная безопасность,

определяемая как состояние защищенности интересов предприятий или организации в информационной сфере. Все направления деятельности предприятия, в которых прямо или косвенно используются информационные технологии, фокусируются в рамках обеспечения информационной безопасности.

Как показывает международная практика, основная проблема в сфере обеспечения информационной безопасности заключается в создании единого эффективного механизма, который позволял бы своевременно применять на практике нормативно-правовые, законодательные акты, отвечающие существующим социально-политическим и экономическим условиям и достижениям в области информационных технологий. Развитие технологий, сферы информатизации делает актуальным вопрос обеспечения информационной безопасности.

Цели и задачи обеспечения информационной безопасности не могут быть отдельно от бизнеса целей и задач организации. Сфера деятельности организации, способы ведения бизнеса, конкурентная среда, применяемые информационные системы, квалификация и мотивация персонала компании, и некоторые прочие факторы изъявляют ключевое воздействие на карту операционных рисков организации, охватывая риски информационной безопасности, а используемые защитные пределы обязаны уменьшать актуальные риски до терпимой величины.

Разбор рисков информационной безопасности позволяет открыть критичные факторы, отрицательно оказывающие влияние на основные бизнес-процессы предприятия, и принимать действенные меры для их устранения или минимизации подобного воздействия. Упущение очень царственной для бизнеса информации в конечном итоге приводит к существенным финансово-экономическим утратам. Не так важно, на какой-либо стадии развития находится информационная система организации, она обязана отвечать установленному комплексу требований к обеспечению информационной безопасности. Имеются требования регуляторов,

свободные от области, а имеются запросы, характерные для установленного сектора экономики. Также имеются «лучшие практики», разрешающие снабдить информационную безопасность на величине, соответствующей целям и запросам данного сегмента бизнеса

Актуальность выбранной темы заключается в том, что информация, бесспорно, выступает основой всего процесса управления в организации, труд управленца и заключается в ее сборе, изучении, обработке и грамотном толковании. От уровня организации сбора, обработки и передачи информации в целом зависит эффективность управления, а также качество принимаемых управленческих решений в частности.

Определённо, самое главное заключается в том то, что информация является, во-первых, предметом, во-вторых средством и в-третьих продуктом труда управленца. Актуальность проблемы заключается в том, что информация может оказывать колоссальное воздействие и на человека, и на технику, как положительное, так и отрицательное, в частности, вызывая у людей неправильное поведение, плохое настроение, а путем установки в компьютере специальных закладок можно извне вывести из строя аппаратуру или прервать ее работу. Но проблема информационной безопасности предприятия, являясь проблематикой, как общей теории организации, так и информационного права, сегодня приобретает новые аспекты. Их появление предопределяется в первую очередь качественными изменениями самого социума и его внешней среды.

Развитие общества, научно-технического прогресса со всей ясностью показывает, что среда обитания человека отнюдь не обладает такими качествами, как прозрачность, определённость, стабильность, что характерно для состояния безопасности в целом и информационной безопасности в частности.

Объектом исследования является ООО «ИнвестПрогрессЛогистик».

Предмет дипломного проекта – процесс обеспечения уровня информационной безопасности предприятия.

Поэтому целью написания данной работы является изучение проблемы обеспечения информационной безопасности предприятия.

Для реализации поставленной цели необходимо решить следующие задачи:

1. Разобраться в сущности информационной безопасности, ее классификациях.

2. Исследовать основные проблемы и угрозы обеспечения информационной безопасности предприятия.

3. Объяснить задачи и уровни обеспечения защиты информации.

4. Предложить проект по обеспечению информационной безопасности предприятия.

Теоретическую и методологическую основу выпускной квалификационной работы составили основные положения экономики, а также концепции, представленные в трудах отечественных и зарубежных ученых по вопросам контроля, законодательные и нормативные акты, стандарты, рекомендации по вопросам экономической безопасности предприятия.

Информационную базу исследования составили государственные и отраслевые стандарты, материалы периодической печати, электронные базы данных и периодические электронные издания в сети Интернет, статистические сборники.

Структура выпускной квалификационной работы определена поставленной целью и последовательностью решения сформулированных задач. Работа состоит из введения, трех глав, заключения, списка используемой литературы и приложения.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

1.1. Интерпретация информационной безопасности

Интерпретация «информационная безопасность» в разных контекстах имеет различное содержание. На сегодняшний день принята Доктрина в аспекте, характуризующем информационную безопасность страны: понятие информационной безопасности применяется в разных смыслах. В основном, характеризуется состоянием защищенности национальных интересов в информационной среде, которые определяются как совокупность сбалансированных интересов личности, общества и государства.

Отметим, что законом Российской Федерации «Об участии в международном информационном обмене» определяется данное словосочетание аналогичным образом и характеризуется состоянием защищенности информационной сферы общества, которое обеспечивает ее формирование, использование и развитие в интересах граждан, предприятий, государства [14].

В последнее время информация стала полноценным фактором производства, наряду с землей, трудом, капиталом и предпринимательскими способностями. Теперь производство сбора, создания, обработки, хранения, анализа и передачи информации пользователю проходит очень сложные этапы, при этом сталкиваясь с различными проблемами. Одна из таких проблем – это обеспечение защищенности информационной составляющей, в том числе и экономической безопасности, сохранение надежности информации, её актуальности, ценности, полноты, достоверности и секретности, а также безопасность самих информационных систем и технологий. Искажение или фальсификация, уничтожение или разглашение информации ведет к разрушению процессов её обработки и передачи в системы, наносят огромный вред как юридическим и физическим лицам, которые участвуют в процессах информационного взаимодействия, так и

государству в целом. Опасным явлением для экономической безопасности является возникновение «инцидента экономической безопасности», т.е. может возникнуть ситуация, представленая нежелательным событием, которое может осуществить нарушение деятельности или экономической безопасности. То есть это те случаи, которые при своем появлении ведут к нарушению экономической безопасности. Природа появления подобного инцидента весьма разнообразна: от случайной ошибки персонала или неправильного функционирования технических средств, влияния природного фактора (пожар, наводнение и т.д.) до преднамеренных злоумышленных действий, которые могут привести к нарушению целостности, секретности, доступности информации и т.д. Все большую опасность обретают внешние угрозы обеспечения защиты информационной составляющей экономической безопасности. Бизнес-пользователи в современном мире не работают в закрытой среде, поэтому их компьютеры подвержены атакам злоумышленников, разносящим вредоносные программы [17].

На основании рассмотренного выше отметим, что информационная безопасность характеризуется состоянием защищенности информационных потоков и поддерживающей инфраструктуры от нежелательных воздействий естественного или искусственного характер. Данные воздействия могут нанести огромный ущерб субъектам информационных отношений, особенно это касается владельцев и пользователей информации и поддерживающей инфраструктуры. Что касается защиты информации, то она может быть представлена как комплекс мер, который направлен на формирование информационной безопасности. Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности можно представмить как оборотную сторону в использовании технологий информационного назначения [19].

Подчеркнем, что трактовка проблем, которые связаны с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае «пусть лучше все сломается, чем враг узнает хоть один секретный бит», во втором – «да нет у нас никаких секретов, лишь бы все работало» [21].

Следует отметить, что информационная безопасность не опирается только на защиту от несанкционированного доступа к информации. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте. Возвращаясь к вопросам терминологии, отметим, что термин «компьютерная безопасность» (как эквивалент или заменитель информационной безопасности) представляется нам слишком узким. Компьютерная система – является одной из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую очередь на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность формирует совокупность составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на «горчичнике», прилепленном к монитору) [15].

Информационная безопасность находится в зависимости не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Данный вид инфраструктуры наполняет самостоятельная ценность, но нас будет

интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций [28].

Отметим, что в определении информационной безопасности перед существительным «ущерб» стоит прилагательное «неприемлемый». Провести страхование от всех видов ущерба невозможно, тем более невозможно осуществить это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Поэтому следует смириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений [41].

Отметим, что информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход. Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры [19].

Выделим главные задачи по обеспечению безопасности:

- осуществление защиты информации в канале связи и базе данных криптографическими методами; осуществление подтверждения подлинности объектов данных и пользователей (аутентификация сторон, которые устанавливают связь);

- обеспечение защиты технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки по побочным каналам и от возможно внедренных в них электронных устройств съема информации; обеспечение защиты программных продуктов и средств вычислительной техники от внедрения в них программных вирусов и закладок;

- защита от несанкционированных действий по каналу связи от лиц, не допущенных к средствам шифрования, но преследующих цели компрометации секретной информации и дезорганизации работы абонентских пунктов [16];

- организационно-технические мероприятия, направленные на обеспечение сохранности конфиденциальных данных.

Иногда в число основных составляющих информационной безопасности включают защиту от несанкционированного копирования информации, но, многие исследователи считают, это слишком специфический аспект с сомнительными шансами на успех. Поясним подробнее основные категории информационной безопасности: понятия доступности, целостности и конфиденциальности.Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность [17].

Наконец, конфиденциальность – это защита от несанкционированного доступа к информации. Изучая информационную безопасность, нельзя не отметить такое понятие, как канал утечки информации – совокупность источника информации, материального носителя, несущих указанную информацию и средства выделения информации из сигнала. Через каналы утечки реализуется угроза конфиденциальности информации, иллюстрация представлена на рисунке 1.1.

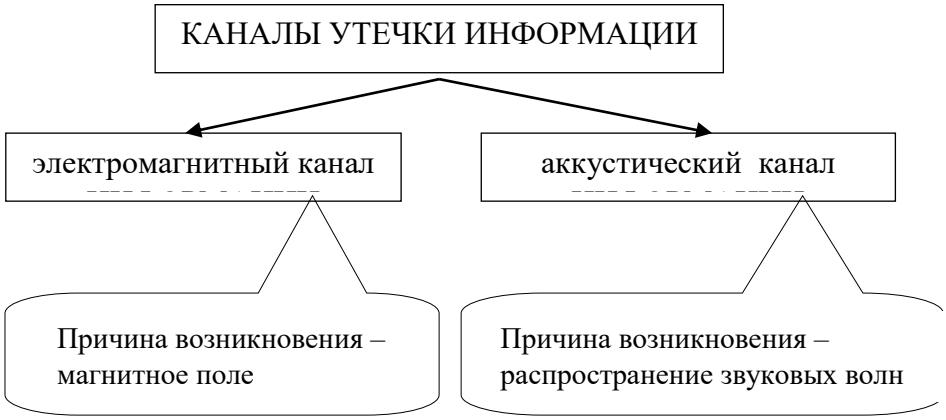


Рисунок 1.1 – Основные каналы утечки информации [20]

Отметим характеристики каналов утечки информации более подробнее:

- электромагнитный канал (причина возникновения - электромагнитное поле, которое связано с протеканием электрического тока в технических система информационных технологий);

- аккустический канал (причина возникновения - распространение звуковых волн в воздухе и упругих средах, которые возникают при работе устройств отображения информации).

Иллюстративно схема общей политики информационной безопасности представлена на рисунке 1.2.

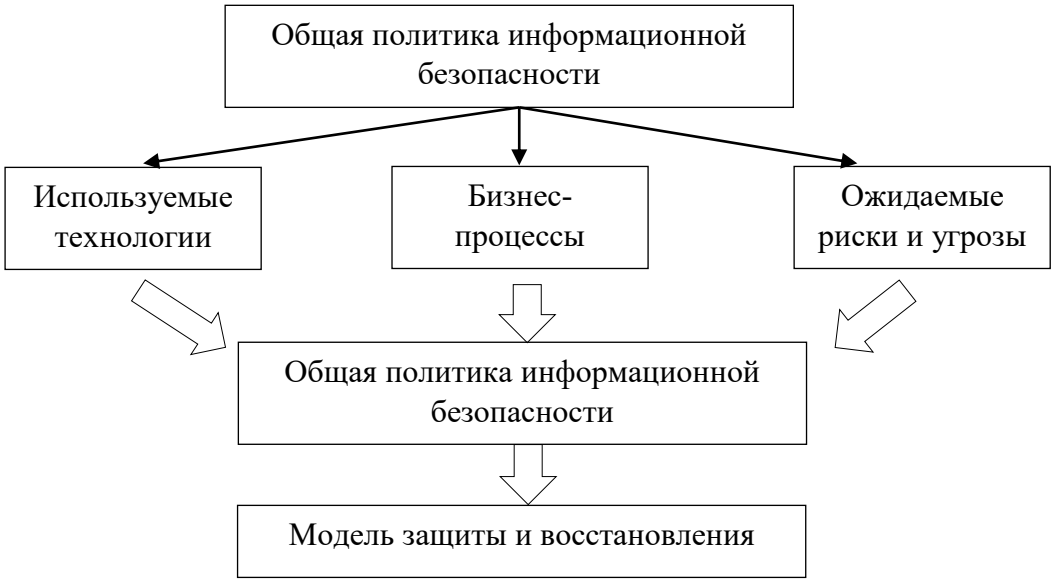


Рисунок 1.2 – Схема организации информационной безопасности

Информационные системы формируются для того, чтобы получить определенные информационные услуги. Если по определнным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, может принести ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важный элемент информационной безопасности [21].

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг,

которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую(относящуюся к корректному выполнению сложных действий(транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений [19].

Целостность оказывается важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации. Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы [18].

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует информационные системы, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения?

Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли). Объектами угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты(персонала, материальных и финансовых ценностей, информационных ресурсов). Угрозы информации выражаются в нарушении ее доступности, целостности и конфиденциальности.Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба [23].

Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкционированного доступа к охраняемым сведениям. Источниками конфиденциальной информации являются люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства. Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности [28].

Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы. Последние могут быть реализованы как аппаратно, программно, так и смешанно-программно-аппаратными средствами. В качестве способов защиты выступают всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие несанкционированному доступу. На рисунке 1.3 представлена концептуальная модель безопасности информации.

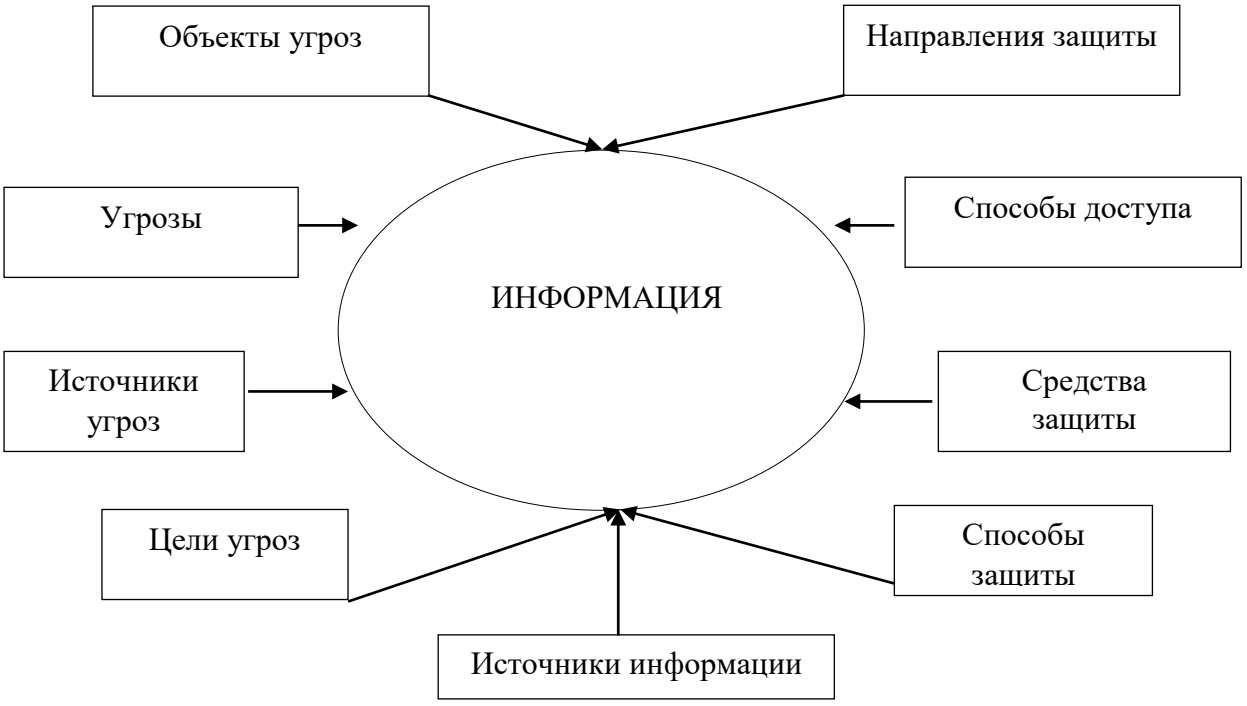


Рисунок 1.3 – Концептуальная модель безопасности информации [33]

Также следует отметить условия, которые способствуют неправомерному овладению конфиденциальной информацией. Современные исследователи указывают следующие условия:

• условие в разглашении или излишней болтливости сотрудников – 32-33%;

• условие в несанкционированном доступе за счет подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок – 24-25 %;

• условие в отсутствии на предприятии условий надлежащего контроля и жестких условий в обеспечении информационной безопасности – 14-15%;

• условие традиционного обмена производственным опытом – 12 %;

• условие бесконтрольного применения информационных систем – 10-11%;

• условие наличия предпосылок по возникновению среди сотрудников конфликтных ситуаций – 8-9%, а также отсутствие высокой трудовой

дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа службы кадров по сплочению коллектива.

Таким образом, в данном параграфе была представлена краткая интерпретация понятия« информационная безопасность»: представляет собой многогранную область деятельности, в которой успех может принести только систематический, комплексный подход. Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить: обеспечение доступности, конфиденциальности информационных ресурсов и поддерживающей инфраструктуры. Рассмотрены основные задачи обеспечения безопасности предприятий; изучены каналы утечки информации ; представлена схема организации информационной безопасности и концептуальная ее модель. Непосредственно, на информационную безопасность любого предприятия оказывают существенную роль ряд угроз и факторов, которые значительным образом влияют в целом на экономическую безопасность предприятия. Их сущность представлена в следующем параграфе.

1.2. Классификация угроз информационной безопасности и способы защиты информации

Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий . Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности. Конечно, проблема утечек появилась не сегодня, промышленный шпионаж и переманивание квалифицированных специалистов существовали еще и до эпохи компьютеризации. Но именно с появлением ПК и интернета возникли новые приемы незаконного получения информации. Если раньше для этого необходимо было украсть и вынести из фирмы целые кипы бумажных документов, то сейчас огромные объемы

важных сведений можно запросто слить на флэшку, помещающуюся в портмоне, отправить по сети, прибегнув к использованию семейства руткитов, троянов, бэкдоров, кейлоггеров и ботнетов, либо просто уничтожить посредством вирусов, устроив диверсию [45].

Представим иллюстративно основные угрозы информационной безопасности на рисунке 1.4.

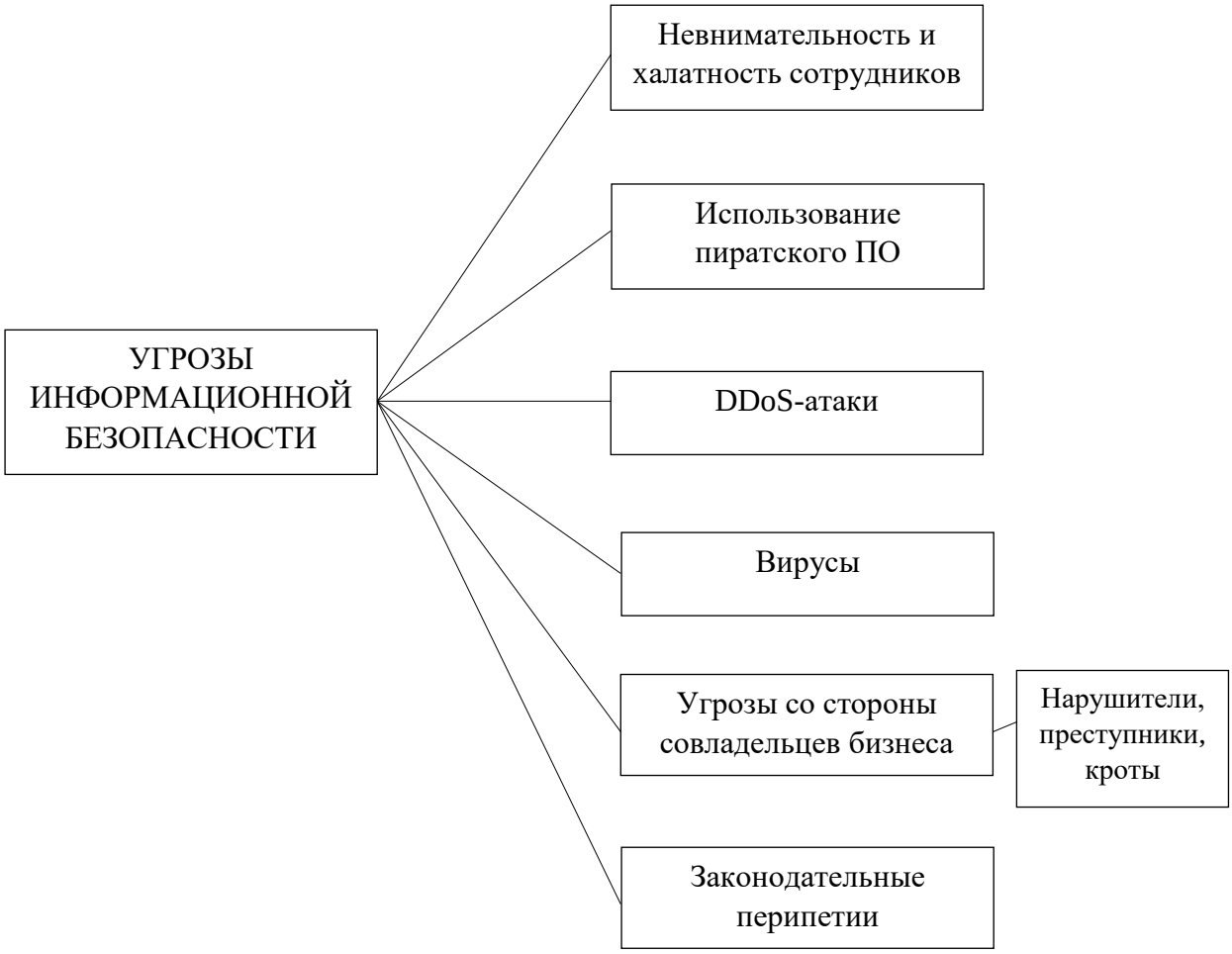


Рисунок 1.4 – Основные угрозы информационной безопасности предприятий

Рассмотрим представленные угрозы информационной безопасности более подробно:

1. Угроза невнимательности и халатности сотрудников: угрозу информационной безопасности предприятия, 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 фирмы. Или, например, скопирует файл с конфиденциальными сведениями на планшет, флэшку для работы в командировке. И ни одна компания не застрахована от пересылки невнимательным сотрудником важных файлов не по тому адресу. В такой ситуации информация оказывается весьма легкой добычей. Приведем пример : 7 лет назад прототип смартфона iPhone 4 был оставлен в баре одним из сотрудников компании Apple Греем Пауэллом. До официальной презентации гаджета оставалось еще несколько месяцев, но нашедший смартфон студент продал его за 5000 долларов журналистам Gizmodo, сделавшим эксклюзивный обзор новинки [31].

2. Угроза применения пиратского программного обеспечения: иногда руководители предприятий пытаются сэкономить на покупке лицензионного программного обеспечения. Но следует знать, что нелицензионные программы не дают защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Обладатель нелицензионного программного обеспечения 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 [35].

В соответствии с принятым в теории и на практике делением нарушений авторских прав на программное обеспечение, можно выделить следующие виды компьютерного пиратства:

– изготовление и/или распространение копий программ без соответствующего разрешения правообладателя;

– непосредственное использование в коммерческой деятельности предприятий нелицензионных копий компьютерных программ,

установленных на рабочие компьютеры сотрудников предприятий/организаций(все виды воспроизведения: запись, хранение в памяти компьютера, эксплуатация программы).

Использование нелицензионного программного обеспечения влечет за собой как административную, так и уголовную ответственность, причем реальные примеры из жизни показывают, что правонарушители несут преимущественно уголовную ответственность [22].

Физические лица, если размер нарушения составил более 50 тысяч рублей, привлекаются к уголовной ответственности, как правило, в виде лишения свободы условно с испытательным сроком и штрафа, а также привлечение к гражданской ответственности и возмещение вреда за нарушение авторских прав.

3. Угроза 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. Мишенью злоумышленников чаще становятся сайты банков, в половине случаев (49%) были затронуты именно они. Приведем пример: в 2016 году DDoS-атаки были зафиксированы в каждом четвертом банке (26%). Среди других финансовых структур вредному воздействию подверглось 22% компаний. Усредненный ущерб для кредитных организаций составил 1 172 000 долларов в расчете на банк [34].

4. Угроза вирусов: одной из самых опасных на сегодняшний день угроз информационной безопасности являются компьютерные вирусы. Это подтверждается многомиллионным ущербом, который несут компании в результате вирусных атак. В последние годы существенно увеличилась их частота и уровень ущерба. По мнению экспертов, это можно объяснить появлением новых каналов проникновения вирусов. На первом месте по-прежнему остается почта, но, как показывает практика, вирусы способны проникать и через программы обмена сообщениями, такие как ICQ и другие. Увеличилось и количество объектов для возможных 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. В последнее время особенно активны стали так называемые вирусы-шифровальщики. Весной и летом этого года миллионы пользователей пострадали от атак вирусов WannaCry, Petya, Misha. Эпидемии показали, что жертвой вирусной атаки можно стать, даже если не открывать подозрительные письма. По информации Intel вирусом WannaCry заразились 530 тысяч компьютеров, а общий ущерб компаний составил более 1 млрд долларов [21].

5. Угрозы со стороны совладельцев бизнеса: именно легальные пользователи – одна из основных причин утечек информации в компаниях. Такие утечки специалисты называют инсайдерскими, а всех инсайдеров условно делят на несколько групп:

- «Нарушители» - среднее звено и топ-менеджеры, которые позволяют себе небольшие нарушения информационной безопасности – играют в компьютерные игры, делают онлайн-покупки с рабочих компьютеров, пользуются личной почтой. Такая безалаберность способна вызвать инциденты, но чаще всего они являются непредумышленными. Кстати, большинство внешних атак происходят именно через личные почтовые ящики или ICQ сотрудников;

- «Преступники»: чаще всего инсайдерами являются топ-менеджеры, имеющие доступ к важной информации и злоупотребляющие своими привилегиями. Они самостоятельно устанавливают различные приложения, могут отсылать конфиденциальную информацию заинтересованным в ней третьим лицам и т.д.;

- «Кроты» - сотрудники, которые умышленно крадут важную информацию за материальное вознаграждение от компании-конкурента. Как правило, это весьма опытные пользователи, умело уничтожающие все следы своих преступлений. Поймать их в силу этого бывает очень непросто. Еще одна категория — это уволенные и обиженные на компанию сотрудники, которые забирают с собой всю информацию, к которой они имели доступ. Обычно украденная информация используется ими на новом месте работы, целенаправленная продажа данных в России пока не слишком актуальна.

6. 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 острейших 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 [47].

Отметим следующую информацию: аналитический центр InfoWatch опубликовал данные по утечке данных в России за 2016 год. Согласно исследованию, СМИ 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 [46].

Подчеркнем, что на сегодняшний день конфиденциальная информация представляет огромный интерес для конкурирующих фирм. Именно она становится причиной посягательств со стороны злоумышленников.

Многие проблемы связаны с недооценкой важности угрозы, в результате чего для предприятия это может обернуться крахом и банкротством. Даже единичный случай халатности рабочего персонала может принести компании многомиллионные убытки и потерю доверия клиентов.

Угрозам подвергаются данные о составе, статусе и деятельности компании. Источниками таких угроз являются:

- конкуренты;
- коррупционеры;
- преступники [24].

Особую ценность для них представляет ознакомление с охраняемой информацией, а также ее модификация в целях причинения финансового ущерба. К такому исходу может привести утечка информации даже на 20%. Иногда потеря секретов компании может произойти случайно, по неопытности персонала или из-за отсутствия систем защиты.

В современных рыночных условиях количество угроз постоянно растет, появляются все новые и новые вирусы, увеличивается интенсивность и частота DDoS-атак, разработчики средств защиты информации тоже не стоят на месте. На каждую угрозу разрабатывается новое защитное программное обеспечение или совершенствуется уже имеющееся. Среди современных способов защиты информации можно выделить:

1. 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.

2. 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.

3. 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.

4. Резервное копирование данных. Это решение, подразумевающее 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. Создать резервную копию и восстановить данные можно в любое удобное для пользователя время, в любой географической точке [39].

5. План аварийного восстановления данных. Крайняя мера защиты информации после потери данных. Такой план необходим каждой компании

для того, чтобы в максимально сжатые сроки устранить риск простоя и обеспечить непрерывность бизнес-процессов. Если компания по каким-то причинам не может получить доступ к своим информационным ресурсам, наличие такого плана поможет сократить время на восстановление информационной системы и подготовки ее к работе. В нем обязательно должна быть предусмотрена возможность введения аварийного режима работы на период сбоя, а также все действия, которые должны быть предприняты после восстановления данных. Сам процесс восстановления следует максимально отработать с учетом всех изменений системы [19].

6. 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 [41].

Отметим основные инструменты обеспечения безопасности корпоративной информации. Количество и изощренность угроз информационной безопасности ежегодно растет. Несмотря на то, что индустрия услуг по защите информации развивается, злоумышленникам иногда все же удается быть на шаг впереди. И происходит это не потому, что нет эффективных средств защиты или квалифицированных консультантов, способных решить проблему. Скорее, это происходит от того, что руководители компаний не до конца понимают необходимость защиты информационных ресурсов. Недостаточно просто установить антивирусные программы и ограничить доступ к тем или иным данным. Чтобы обеспечить максимальную конфиденциальность информации, придется создать многоуровневую систему ее защиты, и далеко не всегда с этой задачей может справиться собственный IT-отдел фирмы. В таком случае на помощь приходят специализированные компании, профессионально занимающиеся

именно защитой информационных ресурсов. Многие фирмы предлагают комплекс эффективных решений по защите данных. Во-первых, это резервное копирование данных Backup-as-a-Service(BaaS) и их хранение в облаке DEAC на базе одного или нескольких дата-центров. Гарантируется полная сохранность информации, а при возникновении клиента форс-мажорных обстоятельств резервные копии помогут в максимально короткие сроки восстановить жизненно важные для компании данные и избежать убытков. Во-вторых, высокий уровень защиты данных, расположенных на инфраструктуре DEAC, вне зависимости от их расположения – как в России, так и в Европе — достигается дополнительно при помощи системы защиты от DDoS-атак. Это система, автоматически определяющая и блокирующая все известные виды DDoS-атак. Применение системы гарантирует непрерывность работы сети клиента и обеспечивает быстрое время отклика на запросы реальных пользователей даже непосредственно во время атаки. И в-третьих, предлагается разработка плана аварийного восстановления(disaster recovery) ИТ-системы с учетом особенностей бизнеса каждой компании, анализируя риски и определяя важнейшие вопросы безопасности на межгосударственном уровне. План включает не только процедуру резервного копирования, но и комплекс действий для обеспечения непрерывного доступа к бизнес-информации компании». Для справки отметим, что дата-центров DEAC вышел на рынок в 1999 году. На сегодня компания имеет 6 отделений – в Лондоне, Амстердаме, Риге, Франкфурте. В штате DEAC работает более 100 высококвалифицированных экспертов, реализованы проекты более чем в 40 странах мира [49].

Следует отметить следующее: разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности. Чаще всего специалисты по безопасности:

- разрабатывают внутреннюю документацию, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;

- проводят инструктаж и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам , где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;
- разграничивают зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;
- внедряют программные продукты, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;
- составляют планы восстановления системы на случай выхода из строя по любым причинам [16].

Группа технических средств защиты информации совмещает аппаратные и программные средства. Основные:

- резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе;
- дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;
- создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
- обеспечение возможности использовать резервные системы электропитания ;
- обеспечение безопасности от пожара или повреждения оборудования водой;
- установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией.Организация информационной безопасности на предприятии

производится таким образом, чтобы хакер мог столкнуться с множеством уровней защиты. В результате злоумышленнику не удаётся проникать в защищённую часть [31].

К наиболее эффективному способу защиты информации относится криптостойкий алгоритм шифрования при передаче данных. Система зашифровывает саму информацию, а не только доступ к ней, что актуально и для безопасности банковской информации. Классификация криптографических алгоритмов представлена на рисунке 1.5.

Рисунок 1.5 – Классификация криптографических алгоритмов [19]

Структура доступа к информации должна быть многоуровневой, в связи с чем к ней разрешается допускать лишь избранных сотрудников. Право полного доступа ко всему объему информации должны иметь только достойные доверия лица.

Отметим, что перечень сведений, касающихся информации конфиденциального характера, утверждается руководителем предприятия. Любые нарушения в этой области должны караться определенными санкциями. Модели защиты предусматриваются соответствующими ГОСТами и нормируются целым рядом комплексным мер. В настоящее время разработаны специальные утилиты, круглосуточно отслеживающие

состояние сети и любые предупреждения систем информационной безопасности.

Во избежание случайных потерь данных по неопытности сотрудников, администраторы должны проводить обучающие тренинги. Это позволяет предприятию контролировать готовность сотрудников к работе и дает руководителям уверенность в том, что все работники способны соблюдать меры информационной безопасности [32].

Атмосфера рыночной экономики и высокий уровень конкуренции заставляют руководителей компаний всегда быть начеку и быстро реагировать на любые трудности. В течение последних 20 лет информационные технологии смогли войти во все сферы развития, управления и ведения бизнеса.

Из реального мира бизнес уже давно превратился в виртуальный, достаточно вспомнить как стали популярны электронные цифровые подписи, у которого имеются свои законы. В настоящее время виртуальные угрозы информационной безопасности предприятия могут насести ему огромный реальный вред. Недооценивая проблему, руководители рискуют своим бизнесом, репутацией и авторитетом [17].

Таким образом, на основании рассмотренного выше отметим, что большинство предприятий регулярно терпят убытки из-за утечки данных. Защита информации предприятия должна занимать приоритетное место в ходе становления бизнеса и его ведения. Обеспечение информационной безопасности – залог успеха, прибыли и достижения целей предприятия. Существует ряд нормативно-правовых актов в области информационной безопасности и защиты информации, суть которых представлена в следующем параграфе.

1.3. Нормативные правовые акты в области информационной безопасности и защиты информации

Информационное законодательство представляет собой совокупность законов, иных нормативно-правовых актов, с помощью и посредствам которых государство устанавливает, изменяет либо прекращает действие соответствующих информационно-правовых норм. Информационное законодательство выступает главенствующей формой закрепления норм информационного права и важнейшим правообразующим фактором. Появление информационного законодательства в системе нормативно-правовых актов РФ свидетельствует о повышении роли государства в регулировании информационных отношений и придании им качества общественно значимых отношений.

Систему информационного законодательства образуют различные законы и издаваемые в соответствии с ними иные нормативные правовые акты, посвященные прямому или опосредованному регулированию отношений, объектом которых является информация, производные от нее продукты и связанная с ними деятельность.

Системы информационного законодательства включают в себя правовые акты федеральных органов и органов субъектов РФ. Среди правовых актов федеральных органов главное место занимают федеральные законы. Они обладают высшей юридической силой, регулируют наиболее важные, основополагающие отношения и содержат информационно-правовые нормы исходного характера, которые рассчитаны на постоянное либо длительное действие.

Нормативные акты, не относящиеся к категории законов, являются подзаконными. В их число входят нормативные акты Президента РФ, Правительства РФ, ведомственные нормативные акты. Многие из них носят комплексный характер, но включают в себя и правила информационно-правового содержания.

Указы Президента РФ – основные акты осуществления компетенции Президента РФ, непосредственно закрепленной в Конституции РФ и вытекающей из основополагающих принципов разделения властей.

Правовые акты Правительства РФ издаются главным образом тогда, когда в законе есть на то прямые указания либо дано конкретное поручение Президента РФ.

Ведомственные акты издаются на основе законов, указов президента и актов правительства. Они представляют собой управленческие акты органов специальной компетенции. Их юридическая сила зависит от функций издавшего их органа и специфики государственного управления информационной сферой. На уровне субъектов РФ применяются все те же формы выражения информационного права, что и на федеральном уровне(законы субъектов РФ, постановления органов исполнительной власти, акты отраслевых и территориальных органов управления).

Наряду с актами законодательства и подзаконными нормативными актами существуют так называемые локальные нормативные акты. Они, как правило, представляют собой приказы и распоряжения нормативного и индивидуального значения, принимаемые руководителями различных организаций. С помощью локальных актов регулируются самые различные информационные вопросы, например, порядок конфиденциального делопроизводства, допуска сотрудников к служебной и коммерческой тайнам порядок организации защиты коммерческой тайны в организации и т. п. [11].

Система по информационному законодательству включает акты международно-правового характера, предметом регулирования являются информационные отношения. На сегодняшний день информационное законодательство проходит этап своего становления, можно смело говорить о наличии некой его упорядоченности. Основа упорядоченности характеризуется принципом иерархии, который выражается в соподчиненности актов различного уровня. Первый уровень, который можно условно назвать конституционным, отражает ведущую роль Конституции в информационно-правовом нормотворчестве. Он представлен рядом конституционных норм. Второму уровню нормативных правовых актов

присущи акты информационного законодательства. Специфика данного уровня состоит в том, что федеральные законы, регулирующие отношения в информационной среде, а равно иные принятые в соответствии с ними нормативные акты подчинены Конституции и не могут ей противоречить.

База среди законов для сферы информации выступает федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который пришел на смену федерального закона от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» [1]. Новый закон регулирует три группы взаимосвязанных между собой отношений, которые складываются:

– в случае осуществления права на поиск, получение, передачу, производство и распространение информации;

– в случае применения информационных технологий;

– в случае обеспечения защиты информационных данных (ЗИ) [1].

К актам информационного законодательства федерального уровня относится и ФЗ от 29.11.1994 № 77-ФЗ «Об обязательном экземпляре документов» является актом по информационному законодательству федерального уровня. Представленный закон позволяет определить политику государства в области по формированию обязательного экземпляра документов как ресурсной базы комплектования библиотечно-информационного фонда РФ и развития системы государственной библиографии, предусматривает обеспечение сохранности обязательного экземпляра документов, его общественное использование. Данным актом установлены виды обязательного экземпляра документации в категории их производителей и получателей, сроки и порядок доставки обязательного экземпляра документов, ответственность за их нарушение [2].

Значимую позицию в рядах законов, регулирующих которые регулируют отношения в информационной сфере, занимает закон РФ от 27.12.1991 № 2124 – 1 «О средствах массовой информации», представляющий собой комплексный нормативный акт, регламентирующий отношения,

возникающие в процессе организации и функционирования средств массовой информации (СМИ) [3].

Особое место среди нормативных актов, регулирующих отношения по поводу информации, принадлежит закону РФ от 21.07.1993 № 5485 – 1 «О государственной тайне» [4].

Один из законов, регулирующих отношения в информационной сфере, – ФЗ от 07.07.2003 № 126-ФЗ «О связи». Он устанавливает правовую основу деятельности в области связи, осуществляемой под юрисдикцией РФ, определяет полномочия органов государственной власти по регулированию этой деятельности, а также права и обязанности физических лиц, осуществляющих деятельность в области связи. К законам, регулирующим информационные отношения, также относится и ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи». Его цель – обеспечение правовых условий использование электронной подписи в электронных документах. Отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников отношений, в том числе государства, на рынке товаров, работ и услуг, регулируются ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [5]. К нормативным актам данной проблематики относятся федеральные законы:

– от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации » [6];

– от 12.05.2009 № 95-ФЗ «О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами» [7]; от 27.07.2006 № 152-ФЗ «О персональных данных» [8]; от 28.12.2010 № 390-ФЗ «О безопасности» [9];

– от 28.07.2012 № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты» [10].

Кроме перечисленных нормативно-правовых актов, существует множество законов, которые непосредственно не направленные на то, чтобы регулировать информационные отношения, но содержащие отдельные статьи, которые посвещены информации или связанные с ней. К ним относятся федеральные законы: от 13.03.2006 № 38 -ФЗ «О рекламе»; от 29.12.1994 № 78-ФЗ «О библиотечном деле»; от 22.10.2004 № 125-ФЗ «Об архивном деле в РФ»; от 17.07.1999 № 176-ФЗ «О почтовой связи»; от 17.08.1995 № 147-ФЗ «О естественных монополиях»; от 21.02.1992 № 2395-1 «О недрах». Определенные нормы, которые касаются информационных отношений, охарактеризованы Гражданским кодексом РФ (ГК РФ). К примеру, статья 150 характеризует личную и семейную тайну, и относит ее к разделу нематериальных благ, статья 726 характеризует обязанности подрядчика о передачи информации заказчику, статья 857 посвящена банковской тайне, статья 946 посвящена тайне страхования. Другая часть гражданского кодекса характеризуется регулированием отношений в области охраны прав на результаты интеллектуальной деятельности.

Среди подзаконных нормативных актов, регулирующих отношения в информационной сфере, можно выделить следующие:

а) указы Президента:

– от 11.02.2006 № 90 «О перечне сведений, отнесенных к государственной тайне»;

– от 06.10.2004 № 1286 «Вопросы межведомственной комиссии по защите государственной тайны»;

– от 17.05.2004 № 611 «О мерах по обеспечению безопасности РФ в сфере международного информационного обмена»;

– от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

– от 15.01.2913 № 31/с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

б) постановления Правительства:

– от 12.02.2003 № 98 «Об обеспечении доступа к информации о деятельности Правительства РФ и федеральных органов исполнительной власти»;

– от 27.05.2002 № 348 «Об утверждении Положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;

– от 22.08.1908 № 1003 «О порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне»;

– от 28.10.1995 № 1050 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне»;

– от 26.10.2012 № 1101 «О создании единой автоматизированной системе« Единый реестр доменных имен, указателей страниц, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети.

Наряду с указами Президента РФ и постановлениями Правительства источниками информационного права выступают акты центральных органов государственного управления РФ (ведомственные нормативно-правовые акты). В области информационных отношений существует значительное их количество. Тематика и направленность данных актов зависит от компетенции издавшего их органа.Так, приказом Федеральной службы безопасности (ФСБ) РФ от 13.11.1999 № 564 утверждено «Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну», которое определяет организационную структуру системы сертификации, порядок проведения сертификации и инспекционного контроля, требования к нормативным и методическим документам по сертификации, а также виды средств защиты информации, подлежащих сертификации.Приказом ФСБ РФ

от 09.02.2005 № 66 утверждено« Положение о разработке, производстве, реализации и эксплуатации шифровальных(криптографических) средств защиты информации)». Важный элемент системы законодательства РФ в информационной сфере – международные соглашения [18].

Таким образом, в данной главе были рассмотрены теоретические основы информационной безопасности. Уточнили, что интерпретация «информационная безопасность» в разных контекстах имеет различное содержание, используется в широком смысле; представлена как состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства или представлена как состояние защищенности информационной среды общества, которое обеспечивает ее формирование, использование и развитие в интересах граждан, организаций, государства. Была изучена классификация угроз информационной безопасности, рассмотрены способы защиты информации, изучены основные нормативно-правовые документы, регулирующие информационную безопасность. В следующей главе рассмотрим особенности информационной безопасности на конкретном примере.

ГЛАВА 2. КОМПЛЕКСНАЯ ОЦЕНКА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ФИРМЫ ООО «ИНВЕСТПРОГРЕССЛОГИСТИК»

2.1. Организационно-экономическая характеристика предприятия

Предприятие «ИнвестПрогрессЛогистик» создано на основании Гражданского Кодекса Российской Федерации. Юридический адрес фирмы: 308002, г. Белгород, проспект Б. Хмельницкого, д. 133, оф. 32-а. Предприятие прошло регистрацию в мае 2011 года Инспекцией Федеральной Налоговой Службы по г. Белгороду.

Основной вид деятельности заключается в вспомогательной и дополнительной транспортной деятельности, организации перевозок грузов.

Наличие собственного современного автопарка и высокий профессионализм сотрудников позволяют фирме обеспечивать качественную, оперативную и безопасную транспортировку грузов по Белгородской области, территории Российской Федерации по конкурентоспособной цене в строго оговоренные сроки. Специалисты фирмы предложат оптимальные маршруты перевозки, исходя из условий и предъявляемых требований.

Также следует отметить, что исследуемая фирма предоставляет услуги по комплексным поставкам различных стриотельных материалов фирмам строительно-дорожной и строительной индустрии на территории Центрального Черноземья(Воронежская область, Курская область, Старый Оскол, Липецк, непосредственно вся территория Белгородчины). Фирма характеризуется достаточным опытом в сотрудничестве со многими крупными строительно-дорожными и строительными предприятиями области. Это говорит о том, что исследуемая фирма наджена и оперативна.

Имущество исследуемогой фирмы представлено основные и оборотными средствами, а также иными материальными ценностями и финансовыми ресурсами. Представим основные источники по созданию имущества ООО «ИнвестПрогрессЛогистик»:

– вложения учредителей материального и денежного характера, основные средства;

– кредитные средства банковских учреждений;

– денежные средства, которые были привлечены юридическими лицами и гражданами;

– безвозмездные или благотворительные взносы, пожертвования предприятий;

– иные источники, не запрещенные законодательными актами.

Фирма« ИнвестПрогрессЛогистик» характеризуется качественным обслуживанием, добросовестно относится к своим клиентам. Представим основные преимущества фирмы:

- наличие квалифицированных опытных водителей;

- специально оборудованный автотранспорт;
- наличие услуг погрузки;
- индивидуальный подход к клиентам;
- оперативное и качественное обслуживание;
- приемлемые цены грузоперевозок;
- профессиональный состав диспетчеров;
- обслуживание сборных грузов;
- юридическая грамотность.

Компания основной своей целью считает создание системы современных услуг перевозок, на уровне мировых стандартов, главными качествами которой являются надежность, профессионализм, безопасность.

Грузовые перевозки осуществляются высококвалифицированными водителями при участии профессионального диспетчера. Водители компании выступают в качестве экспедиторов, что позволяет нести полную материальную ответственность перед клиентами за принятый к перевозке груз. ООО «ИнвестПрогрессЛогистик» самостоятельно прогнозирует перспективы развития на основании конъюнктуры рынка, распоряжается прибылью, которая остается после уплаты налогов и других обязательных платежей. Непосредственно, ООО «ИнвестПрогрессЛогистик» заключает договора с заказчиками и потребителями. Одним из наиболее важных моментов в процессе организации грузовых перевозок предприятием ООО «ИнвестПрогрессЛогистик» является подписание договора о грузоперевозке. На сегодняшний день договор – важная часть предоставления услуг. Согласно договору о грузоперевозке одна сторона, именуемая заказчиком, поручает, а вторая (исполнитель) принимает на себя организацию перевозки грузов, а также осуществление погрузо-разгрузочных работ. В отдельных случаях в подобный договор могут быть включены и некоторые другие виды услуг, в зависимости от желания заказчика и возможностей исполнителя. Продолжительность работы автомобиля на предприятии составляет 8 часов, на некоторых маршрутах работа

организована в два дня, так как груз не удается перевезти за время смены. Подчеркнем, что на исследуемой фирме в начале 2016 года произошло списание трех автотранспортных средств, общая грузоподъемность уменьшилась в 2016 году. В 2015 году коэффициент использования грузоподъемности снизился и равен 1,18. Это означает, что машины идут с некоторым перегрузом. Следовательно, на предприятии преобладают маршруты с обратным холостым пробегом. Среднее расстояние перевозок увеличилось в 2016 году. В основном на предприятии при перевозке грузов задействованы автомобили Камаз, также имеется такой вид транспорта, как газель. Оценка технической оснащенности ООО «ИнвестПрогрессЛогистик» представлена в таблице 2.1.

Таблица 2.1 – Оценка технической оснащенности предприятия

Наименование техники при перевозке грузов	**Годы**			**Абсолютное отклонение (+,-)**	
	2016	**2017**	**2018**	**2017 г. / 2016 г.**	**2018 г. / 2017 г.**
Газель, ед.	10	9	11	- 1	+ 2
Камаз, ед.	6	5	10	- 1	+ 5
Итого техники, ед.	16	14	21	- 2	+ 7

В результате представленной таблицы за 2016-2017 гг мы наблюдаем тенденцию снижения количества имеющейся техники: так в 2017 году число газелей в сравнении с 2016 годом снизилось на 1 единицу, а за весь рассматриваемый период произошло увеличение данного вида на 1 единицу.

Число единиц камазов в 2017 году снизилось на 1 единицу, а в 2018 году наблюдается положительная тенденция: по сравнению с 2017 годом увеличение произошло на 5 единиц (что объясняется заключением партнерских контрактов по перевозке грузов на территории страны). Представим на рисунке 2.1 тенденцию изменения имеющейся техники за 2016-2018 годы фирмы ООО «ИнвестПрогрессЛогистик».

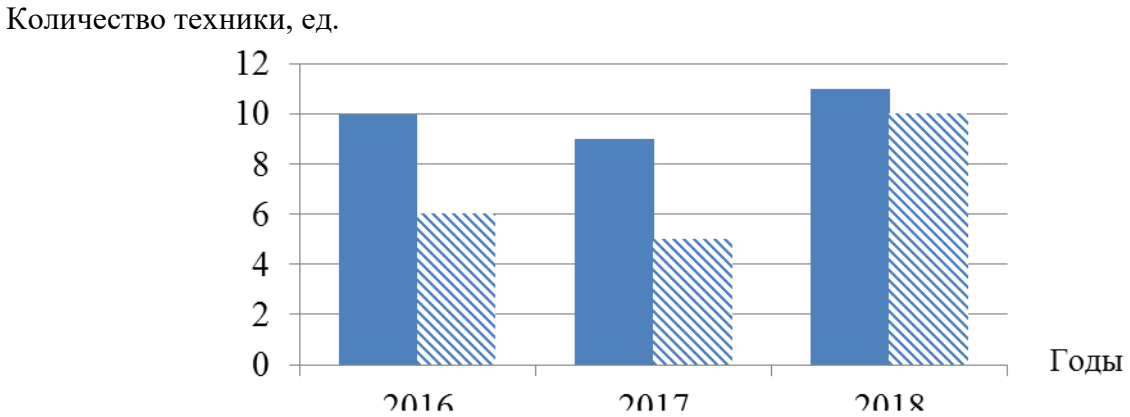


Рисунок 2.1 – Динамика изменения техники ООО ИнвестПрогрессЛогистик» за 2016-2018 гг.

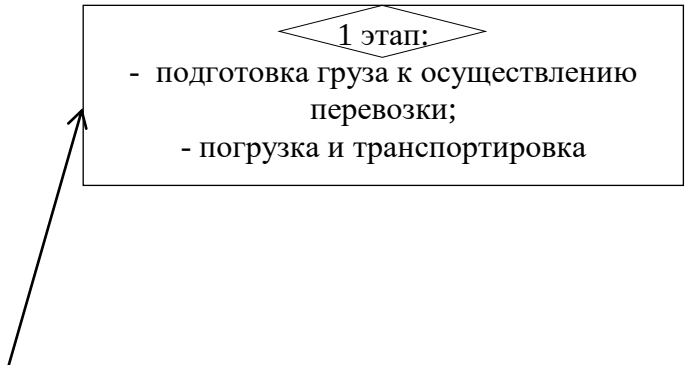
Представим схематично на следующем рисунке 2.2 технологический процесс оказания услуг по перевозке грузов.

I – грузообразующий пункт; II – грузопоглащающий пункт; III – перевозочный комплекс

III
грузопоток перевозочного комплекса; транспортная продукция; потребности грузополучателя; плановая провозная возможность комплекса ; фактическая провозная возможность перевозочного комплекса; операторы

Рисунок 2.2 – Орг ИнвестПрогрессЛогистик»

Подчеркнем: ами принято называть предприятия и ор ного хозяйства, с которых вывозятся их пр поглащающими пунктами понимаются предприятия и организации всех отраслей народного хозяйства, на которые завозятся сырье, топливо, материалы, готовая продукция и другие грузы, необходимые для их нормальной производственной деятельности. Исследуемая фирма ООО «ИнвестПрогрессЛогистик» на перспективу развития своей предпринимательской деятельности формирует методологическую стратегию, суть которой заключается в том, что основной составляющей частью перевозок должно стать проектирование оптимального перевозочногопроцесса. Исследуя данную организацию, также следует уделить внимание схеме технологического процесса оказания услуг, которая представлена на рисунке 2.3.



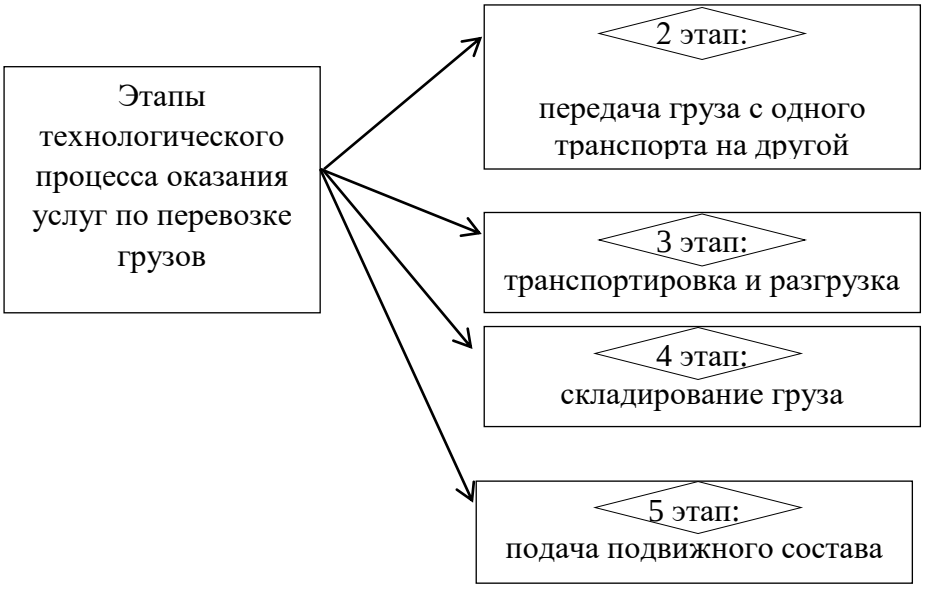


Рисунок 2.3 – Этапы технологического процесса по перевозке грузов

Отметим, что основными конкурентами предприятия ООО «ИнвестПрогрессЛогистик» являются: ООО «Деловые линии»; ООО «МеталлТранзит»; ООО «Автолайн»; ООО «Автобан», механизм взаимодействия представлен на рисунке 2.4.

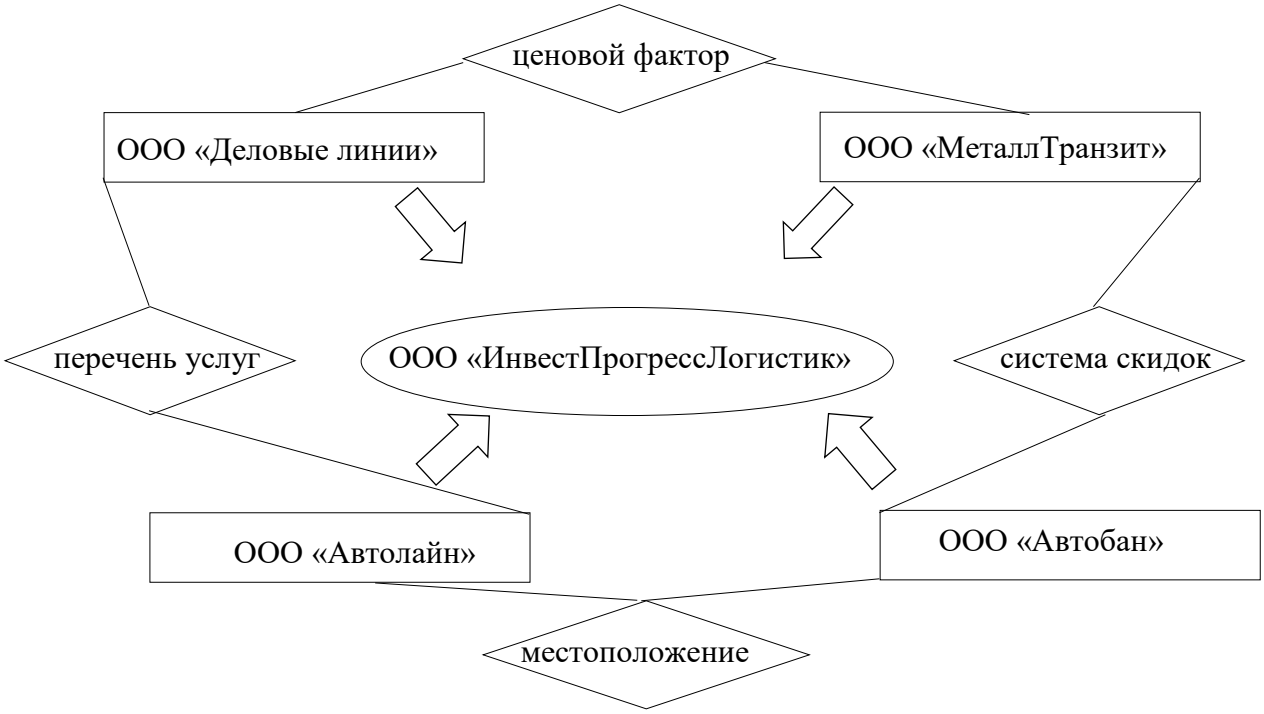


Рисунок 2.4 – Основные конкуренты фирмы с учетом факторов конкуренции

Представленные фирмы являются конкурентами ООО «ИнвестПрогрессЛогистик» по оказываемым видам деятельности, расположению и стажу. Однако на территории Белгорода зарегистрировано

78 прямых грузовладельца, которые также хотят активно функционировать на территории грузоперевозок. Наличие большого числа конкурентов – одна из угроз экономической безопасности фирмы.

Что касается организационной структуры управления, то она устанавливается исходя из целей деятельности и необходимых для достижения этих целей подразделений, выполняющих функции, составляющие бизнес-процессы предприятия. Далее представим организационную структуру управления фирмы ООО «ИнвестПрогрессЛогистик» на рисунке 2.5.

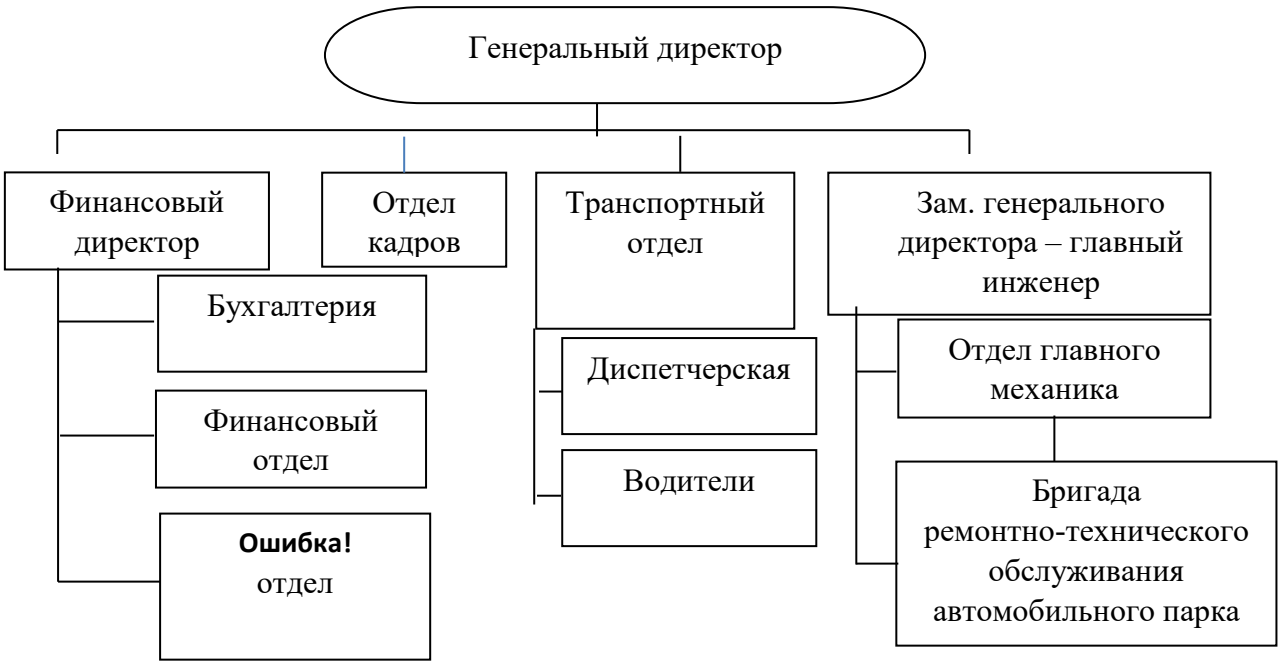


Рисунок 2.5 – Организационная структура ООО «ИнвестПрогрессЛогистик»

Численность сотрудников на начало 2019 года составляет 55 человек. Во главе фирмы ООО «ИнвестПрогрессЛогистик» директор – Алешкин А.А., который является и учредителем. Директор занимается координирование и контролем деятельности подразделений предприятия, принимает решения по всем вопросам деятельности фирмы в пределах своей компетенции, определяемой уставом.

Бухгалтерия ведет бухгалтерскую отчетность на предприятии; осуществляет контакты с банком, налоговыми органами; начисляет

заработную плату работникам предприятия. Главный инженер ООО «ИнвестПрогрессЛогистик» руководит работой ремонтных и производственных служб, хотя принятие решения об оплате материалов для ремонта, запасных частей, оборудования и оплата услуг сторонних организаций остается за директором.

Отдел кадров ООО «ИнвестПрогрессЛогистик» - структура в организации, занимающаяся управлением персоналом. Цель отдела кадров состоит в том, чтобы способствовать достичь целей предприятия путем обеспечения ее необходимыми кадрами и эффективного использования их квалификации, опыта, мастерства, работоспособности, творческого потенциала.

Транспортный отдел является самостоятельным структурным подразделением ООО «ИнвестПрогрессЛогистик». Отдел создается и ликвидируется приказом директора предприятия. Данный отдел подчиняется непосредственно директору ООО «ИнвестПрогрессЛогистик», его возглавляет начальник, назначаемый на должность приказом директора предприятия. Транспортному отделу подчиняются водители и сотрудники мастерской по ремонту машин. Тип представленной организационной структуры – линейно-функциональный. Основное ее достоинство – директор фирмы делегирует полномочия функциональным руководителям. Каждый работник имеет свою должностную инструкцию. В должностной инструкции прописаны общее положение о профессии, обязанности работника, его права и ответственность. При организации работы грузоперевозок фирмой важным аспектом является мобильная, квалифицированная работа сотрудников, способных организовать процесс обслуживания клиентов как можно быстрее и качественней. В обязанности работника транспортного отдела входят следующие функции:

1) контроль поступивших в распоряжение фирмы машин;
2) изменение статуса машин и водителей;
3) удаление информации из базы данных о списанных машинах;

4) сохранение информации о перевозимом грузе;

5) регистрация клиентов, обратившихся в фирму;

6) заполнение накладных поездок.

Деятельность работника транспортного отдела фирмы грузоперевозок – это процесс, происходящий во времени, который можно разделить на последовательные этапы:

1) этап формирования списков машин и водителей;

2) этап оформления документов клиента;

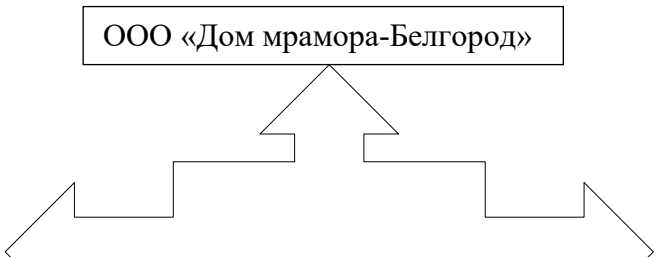
3) этап оформления аренды машины; этап выдачи информации о поездки.

Большую роль в функционировании предприятия и дальнейшей его деятельности играют конкуренты. Основные конкуренты рассматриваемой организации ООО «ИнвестПрогрессЛогистик» следующие:

1) ООО «Деловые линии» (экспресс-доставка корреспонденции и грузов по России изарубежью; курьерские, транспортно-экспедиционные услуги; адресная и безадресная доставка по городу и области);

2) ООО «Автобан»(автотранспортная компания, специализируется на оказании услуг перевозки крупногабаритных и тяжеловесных грузов автомобильным транспортом, услуги перевозки как по городу Белгород, Белгородскойобласти, так и за их пределами, из Центрального Черноземья вСеверо-Западный, Центральный, Южный, федеральные округа и обратно, а также по многим другим направлениям по территории РФ);

3) ООО «Автолайн» (перевозка грузов как по городу Белгороду, Белгородской области, так и за ихпределами, из Центрального Черноземья в Северо-Западный, Центральный, Южный федеральные округа и обратно). ООО «ИнвестПрогрессЛогистик» при осуществлении своей деятельности заключает контракты с определенными фирмами. Основные партнеры фирмы иллюстративно представлены на рисунке 2.6.



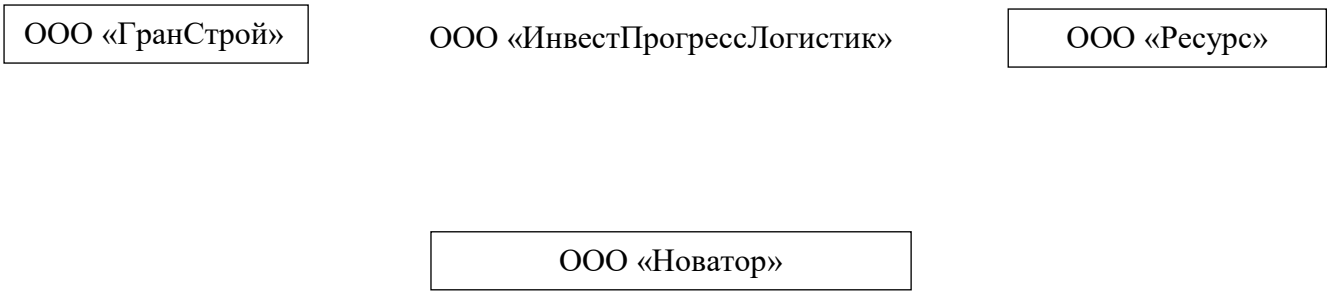


Рисунок 2.6 – Основные партнеры ООО «ИнвестПрогрессЛогистик»

Далее рассмотрим технико-эксплуатационные показатели транспортных перевозок, которые представлены в таблице 2.2.

Таблица 2.2 – Технико-эксплуатационные показатели транспортных перевозок ООО «ИнвестПрогрессЛогистик» за 2016-2018 гг.

Показатели	**2016 г.**	**2017 г.**	**2018 г.**
Объем всехперевозок, тыс. т	314	398,5	401,3
Грузооборот, тыс. т-км	98062	97421	97121
Общий пробег, тыс. км	16573	19875	25432
Среднее расстояние перевозки, км	312	244	289
Коэффициент использования пробега	0,57	0,58	0,61
Коэффициент использования парка	0,55	0,52	0,52
Коэффициент использования грузоподъемности	1,19	1,19	1,20
Коэффициент использования рабочего времени	0,83	0,83	0,82
Средняя техническая скорость, км/ч	25,5	26,0	26,0
Время простоя под погрузкой / разгрузкой за поездку, час	1,4	1,4	1,4
Выработка на 1автотонну, т	122,1	133,2	135,6
Продолжительность работы в сутки, час	12,1	12,2	12,3
Средняя грузоподъемность, т	21,4	18,7	19,4
Среднесуточный пробег, км	277	285	296
Коэффициент выхода автомобилей на линию	3,7	0,7	0,9

На основании представленных данных наблюдается тенденция увеличения объема всех первозок за исследуемый период. Грузооборот имеет тенденциюснижения. На рисунке 2.7 приведен объем перевозок ООО «ИнвестПрогрессЛогистик».

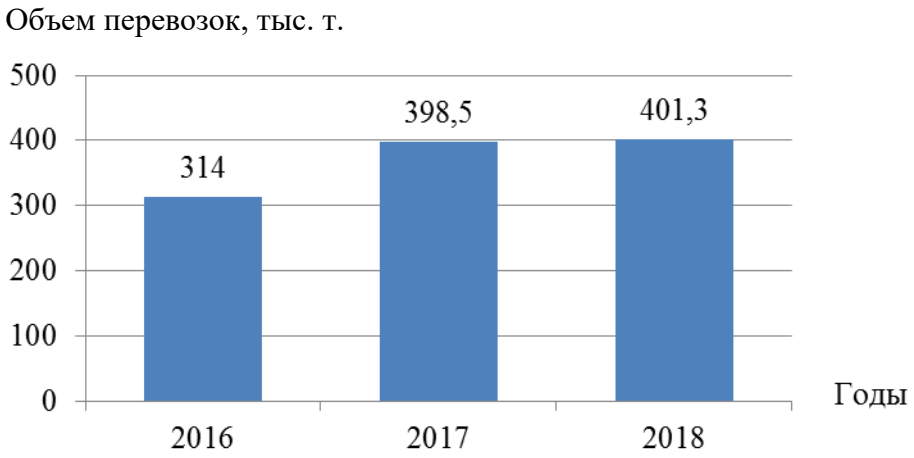


Рисунок 2.7 – Объем перевозок предприятия за исследуемый период

Следует подчеркнуть, что основными клиентами ООО «ИнвестПрогрессЛогистик» выступают предприятия разных отраслей, такие как:

– сельскохозяйственные;

– строительные;

– дорожно-ремонтные;

– промышленные;

– жилищно-коммунальные предприятия Черноземья и других регионов РФ, а также индивидуальные предприниматели и частные лица.

Основными задачами ООО «ИнвестПрогрессЛогистик» при работе с клиентами выступают:

1) удовлетворить потребности заказчика в автомобильных перевозках;
2) обеспечить высокий уровень обслуживания заказчиков;
3) выполнить существующие планы перевозок;
4) эффективно использовать транспортные средства.

Также исследуемая фирма ставит задачи по организации движения подвижного состава в междугородном сообщении:

1) обеспечить количественную и качественную сохранность грузов;

2) обеспечить доставки грузов от отправителя в определенные сроки;

3) максимально использовать грузоподъемности подвижного состава фирмы; повысить оборачиваемость подвижного состава за счет сокращения

простоев в пунктах получения и сдачи грузов и рационального использования времени в пути; обеспечение нормальных условий труда водителей;

4) организация своевременного и качественного технического обслуживания и ремонта подвижного состава, технической помощи и снабжения эксплуатационными материалами.

Рассматривая организационно-экономическую характеристику предприятия, следует особое внимание уделить основным финансовым результатам деятельности фирмы, которые представлены в таблице 2.3.

Таблица 2.3 – Основные экономические показатели деятельности предприятия ООО «ИнвестПрогрессЛогистик» за 2016-2018 гг

Наименование показателя	**Значение показателя, тыс. руб.**			**Изменение показателя 2018 г. / 2016 г.**	
	2016 г.	**2017 г.**	**2018 г.**	**тыс. руб.**	**± %**
Выручка, тыс. руб.	33133	38456	46822	+13 689	+41,3
Расходы по обычным видам деятельности, тыс. руб.	32830	37651	35398	+2 568	+7,8
Прибыль от продаж, тыс. руб.	303	805	11424	+11 121	+3670,3
Прочие доходы и расходы, кроме процентов к уплате, тыс. руб.	1029	- 505	-621	-1 650	- 160,3
Прибыль до уплаты процентов и налогов,	1332	300	10803	+9 471	+711,0
Изменение налоговых активов и обязательств, тыс. руб.	330	161	2160	-1 830	- 554,5
Чистая прибыль, тыс. руб.	1002	139	8 642	+7 640	+99,2
Совокупный финансовый результат периода, тыс. руб.	1002	139	8 642	+7 640	+99,2

На основании представленной таблицы показатель выручки в 2018 году составил 46822 тыс. руб., что на 13689 тыс. руб. больше, чем за 2016 год. Тенденция увеличения выручки за весь анализируемый период составила 41,3%. Расходы по обычным видам деятельности в 2018 г. по сравнению с предыдущим годом снизились на 2253 тыс. руб., что является положительным моментом в развитии деятельности предприятия; по

сравнению с 2016 годом значение данного показателя увеличилось на 2568 тыс. руб. или на 7,8%.

Показатель прибыли от продаж предприятия ООО «ИнвестПрогрессЛогистик» за исследуемый период характеризуется тенденцией увеличения, что является положительным моментом в деятельности исследуемой фирмы. Это объясняется тем, что ООО «ИнвестПрогрессЛогистик» заключило дополнительные контракты на оказание услуг: за рассматриваемый период прибыль увеличилась на 11121 тыс. руб. Совокупный финансовый результат за исследуемый период увеличился на 8 642 тыс. руб. или на 99,2%, иллюстративно представлен на рисунке 2.8.

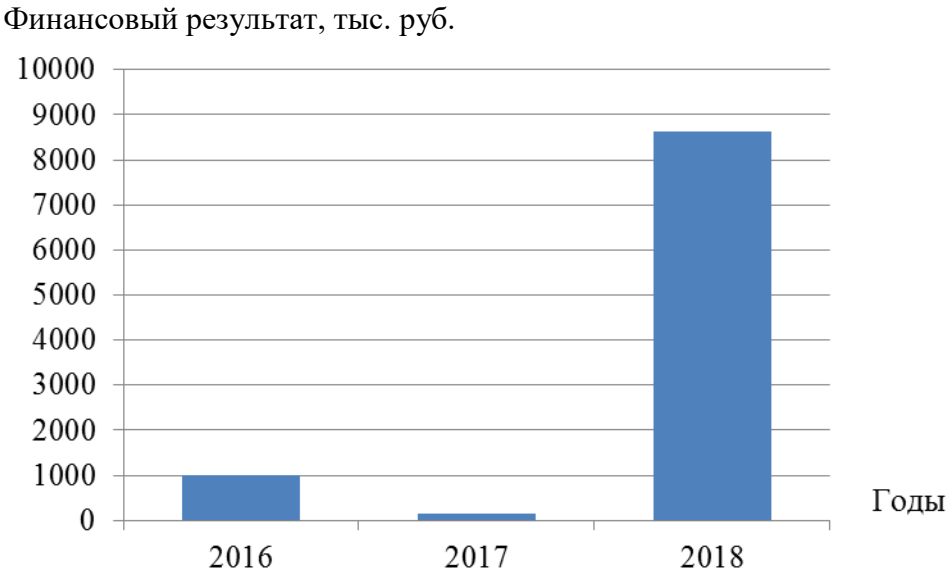


Рисунок 2.8 – Структура совокупного финансового результата предприятия ООО «ИнвестПрогрессЛогистик» за 2016-2018 гг.

Представленная ситуация объясняется снижением расходов, увеличением числа заключения контрактов. Таким образом, на основании рассмотренного выше отметим следующее: исследуемое предприятие ООО «ИнвестПрогрессЛогистик» создано в соответствии с Гражданским Кодексом РФ; местоположение фирмы: г. Белгород, пр-т Б.Хмельницкого, д. 133, оф. 325. Основным видом деятельности выступает вспомогательная и дополнительная транспортная деятельность, организация перевозок грузов. Численность сотрудников на конец отчетного периода составляет 55 человек.

В результате рассмотренных экономических показателей прослеживается увеличение чистой прибыли, что является положительной ситуацией для дальнейшего развития предприятия ООО «ИнвестПрогрессЛогистик». Анализ и оценка экономической безопасности фирмы представлена в следующем параграфе.

2.2. Анализ системы экономической безопасности предприятия

Чтобы провести анализ системы экономической безопасности предприятия, проанализируем финансовый блок (или анализ финансового состояния) процесса оценки финансово-экономического состояния предприятия (набор универсальных показателей, рассчитываемых на базе основных форм бухгалтерской отчетности).

К основным аспектам данного анализа показателей, которые необходимо оценить, относятся: анализ ликвидности и платежеспособности; анализ финансовой устойчивости; анализ деловой активности; анализ эффективности деятельности предприятия. Рассмотрим показатели динамики и структуры актива и пассива исследуемой фирмы.

Актив баланса содержит сведения о размещении капитала, имеющегося в распоряжении предприятия. Сведения, которые приводятся в пассиве баланса, позволяют определить, какие изменения произошли в структуре собственного и заемного капитала, сколько привлечено в оборот предприятия долгосрочных и краткосрочных средств, то есть пассив показывает, откуда взялись средства, направленные на формирование имущества предприятия.

Финансовое состояние предприятия (совокупность показателей, отражающих его способность погасить свои долговые обязательства; экономическая категория, отражающая состояние капитала в процессе его кругооборота и способность субъекта хозяйствования к погашению долговых обязательств и саморазвитию на фиксированный момент времени) ООО

«ИнвестПрогрессЛогистик» во многом зависит от того, какие средства оно имеет в своем распоряжении и куда они вложены. Необходимость в собственном капитале обусловлена требованиями самофинансирования предприятий. В таблице 2.4 представлены данные для анализа динамики и структуры активов и пассивов фирмы.

Таблица 2.4 – Оценка показателей для анализа динамики и структуры активов и пассивов предприятия« ИнвестПрогрессЛогистик»

Наименование показателя	**Годы**			**Абсолютное отклонение (+,-)**	
	2016	**2017**	**2018**	**2017 г. / 2016 г.**	**2018 г. / 2016 г.**
I Активы					
Нематериальные активы	0	0	0	-	-
Основные средства	12096	12618	11350	+ 522	-746
Долгосрочные и краткосрочные финансовые вложения	220	7544	6551	+ 7324	+6331
Запасы	5890	13987	14239	+ 8097	+8349
Налог на добавленную стоимость	23	95	103	+ 72	+80
Дебиторская задолженность	8829	13860	7955	+ 5031	-874
Денежные средства	5763	4971	5430	- 792	-333
Прочие оборотные активы	217	618	977	+ 401	+760
Итого активы, принимаемые к расчету	33 038	53 693	46605	+ 20655	+ 13567
II. Пассивы					
Долгосрочные обязательства по займам и кредитам	628	12427	17455	+ 11799	+16827
Прочие долгосрочные обязательства	0	0	3887	-	+3887
Краткосрочные обязательства по займам и кредитам	0	0	0	-	-
Кредиторская задолженность	29198	37265	23293	+ 8003	- 5905
Прочие краткосрочные обязательства	0	0	0	-	-
Итого пассивы, принимаемые к расчету	29826	49692	44635	+ 19866	+ 59444
Стоимость чистых активов	3212	4001	1970	+ 789	-1242

На основании оценки показателей для анализа структуры активов и пассиов предприятия (целью структурного анализа является изуче-ние структуры и динамики средств предприятия и источников их формирования

для ознакомления с общей картиной финансового состояния), проведем в следующей таблице 2.5 анализ структуры активов и пассивов исследуемой фирмы.

Таблица 2.5 – Анализ структуры активов и пассивов предприятия

Показатель	**Значение показателя**				
	тыс. руб.			**в % к валюте баланса**	
	2016 г.	**2017 г.**	**2018 г.**	**2017 г.**	**2018 г.**
Актив					
Внеоборотные активы	12316	20162	17901	38	38,4
- основные средства	12096	12618	11350	24	24,4
- нематериальные активы	-	-	-	-	-
Оборотные активы, всего	20722	33531	28704	62	61,6
- запасы	5890	13987	14239	26	31
- дебиторская задолженность	8829	13860	7955	26	17,1
- денежные средства и краткосрочные финансовые вложения	5763	4971	5430	9,6	12
Пассив					
Собственный капитал	3212	700	1970	6,3	4
Долгосрочные обязательства, всего	628	12427	21342	23,4	46
- заемные средства	628	12427	17455	23,4	37,5
Краткосрочные обязательства	29198	37265	23293	70,3	50
Валюта баланса	33038	53693	46605	100	100

На основании полученных данных наблюдается следующее:

в 2017 году внеоборотные активы увеличились по сравнению с предыдущим годом, а в 2018 году произошло их снижение. В 2017 году в активах исследуемой фирмы внеоборотные активы занимают долю баланса

в размере 38%. Данную группу возглавила статья« основные средства»:

в процентах к валюте баланса она составила 24%. Снижение внеоборотных активов обусловлено снижением показателя основных средств. Нематериальные активы у предприятия отсутствуют. Структура изменения внеоборотных активов представлена на рисунке 2.9.

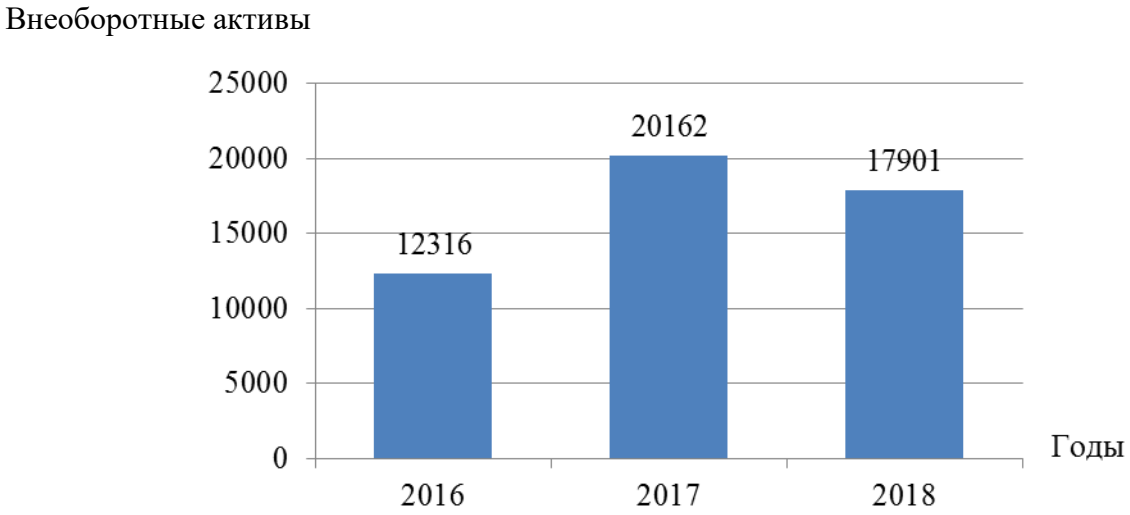


Рисунок 2.9 – Структура внеоборотных активов фирмы за 2016-2018 гг.

Оборотные активы занимают в размере 62 % баланс предприятия. Запасы за исследуемый период характеризуются увеличением; дебиторская задолженность в 2018 году снизилась и составила 7955 тыс. руб. в 2017 году структура оборотных активов увеличилась и составила 33531 тыс. руб. за счет увеличения запасов и дебиторской задолженности. В 2018 году дебиторская задолженность снизилась, и это выступило причиной снижения оборотных активов предприятия. Структура оборотных активов представлена на рисунке 2.10.

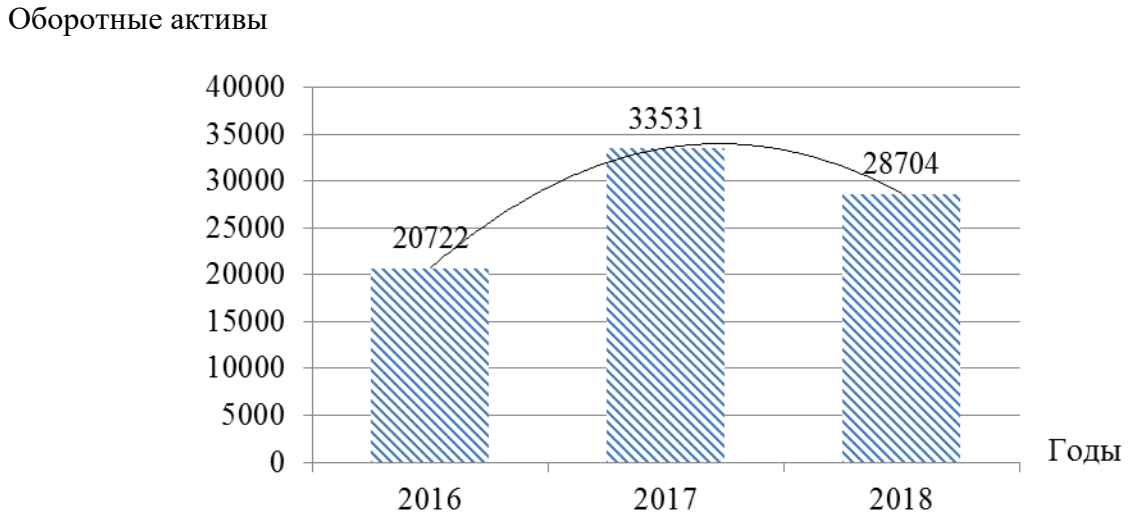


Рисунок 2.10 – Тенденция изменения оборотных активов предприятия

70,3 % в валюте баланса составляют краткосрочные обязательства;

23,4 % – заемные средства; остальной приходится на собственный капитал.

Отметим, что за рассматриваемый период наблюдается рост активов баланса за весь рассматриваемый период:

1) запасы на 9088 тыс. руб. (24,3%);

2) дебиторская задолженность на 8805 тыс. руб. (23,5%);

3) основные средства на 7120 тыс. руб. (19%);

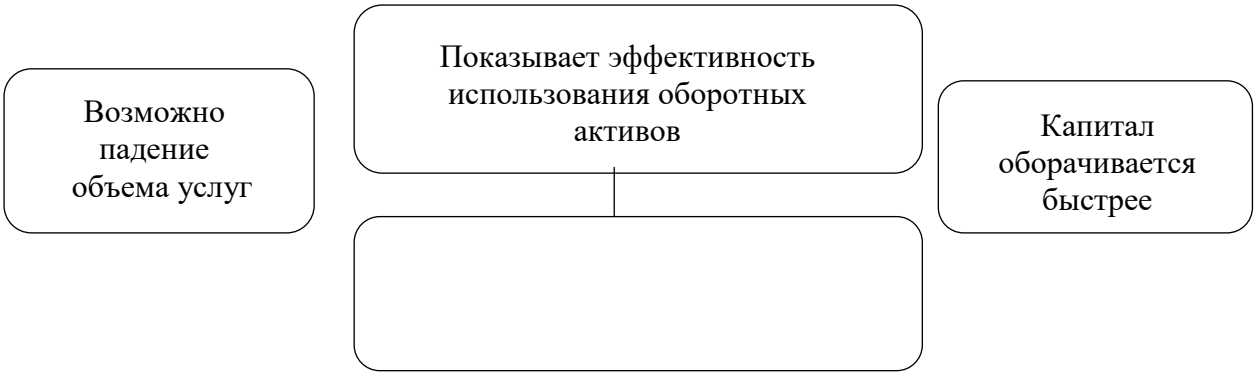
4) краткосрочные финансовые вложения на 6925 тыс. руб. (18,5%).

Одновременно, в пассиве баланса прирост наблюдается по следующим строкам:

1) кредиторская задолженность на 21475 тыс. руб. (59,6%);

2) долгосрочные заемные средства на 12094 тыс. руб. (33,6%);

3) нераспределенная прибыль (непокрытый убыток) на 2443 тыс. руб. (6,8%). Отметим особенности оборачиваемости активов на рисунке 2.11.



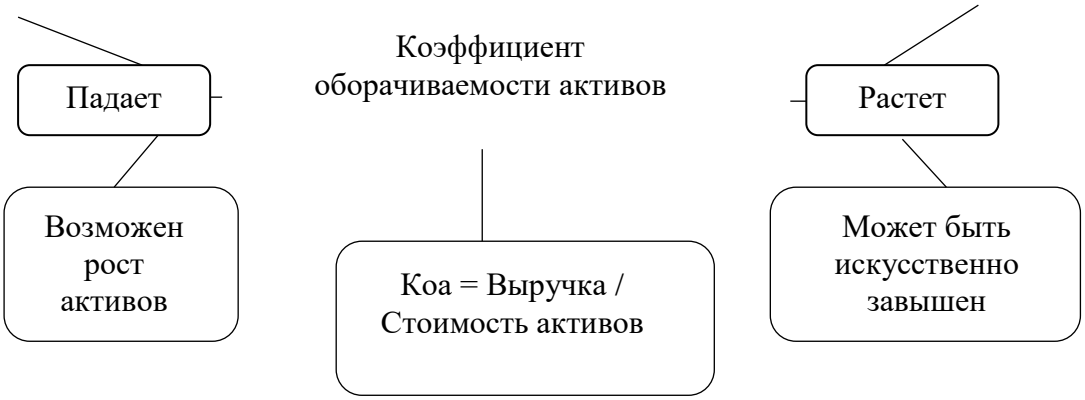


Рисунок 2.11 – Схема коэффициента оборачиваемости активов

На конец анализируемого периода собственный капитал фирмы ООО «ИнвестПрогрессЛогистик» составлял 3351 тыс. рублей.

За исследуемый период данный показатель значительно вырос на 2443 тыс. рублей.

Следующим моментом в анализе системы экономической безопасности предприятия ООО «ИнвестПрогрессЛогистик» является определение финансовой устойчивости. Представим данные и расчет показателей, характеризующих финансовую устойчивость фирмы

ООО «ИнвестПрогрессЛогистик» в таблице 2.6.

Таблица 2.6 – Данные и расчет показателей, характеризующих экономическую безопасность предприятия ООО «ИнвестПрогрессЛогистик» за 2016-2018 гг.

Показатели	**2016 г.**	**2017 г.**	**2018 г.**
Реальный собственный капитал	908,00	3212,00	3351,00
Внеоборотные активы	7503,00	12316,00	13237,00
Оборотные активы	9528,00	20722,00	40456,00
Наличие собственных оборотных средств	-6595,00	-9104,00	-9886,00
Долгосрочные пассивы	333,00	628,00	12427,00
Наличие долгосрочных источников формирования запасов	-6262,00	-8476,00	2541,00
Краткосрочные кредиты и заемные средства	0,00	0,00	0,00
Общая величина основных источников формирования запасов	-6262,00	-8476,00	2541,00
Общая величина запасов (включая неписанный НДС)	4346,00	6130,00	14700,00
Излишек (+) или недостаток (-) собственных оборотных средств	-10941,00	-15234,00	-24586,00

Излишек (+) или недостаток (-) долгосрочных источников формирования запасов	-10608,00	-14606,00	-12159,00
Излишек (+) или недостаток (-) основных источников формирования запасов	-10608,00	-14606,00	-12159,00
Коэффициент маневренности	-7,26	-2,83	-2,95
Коэффициент автономии источников формирования запасов	-1,52	-1,49	-0,67
Коэффициент обеспеченности собственными оборотными средствами	-0,69	-0,44	-0,24
Коэффициент автономии	0,05	0,057	0,06
Коэффициент покрытия инвестиций	0,07	0,1	0,3
Коэффициент обеспеченности запасов	- 1,59	-1,1	-0,75

Она во многом определяет финансовую независимость организации. Также данный показатель является значением платежеспособности

в длительном промежутке времени. В отличие от кредитоспособности является показателем, важным не внешним, а внутренним финансовым службам. На основании представленных данных наблюдается положительная тенденция в формировании реального собственного капитала, тенденция изменения представлена на рисунке 2.12.

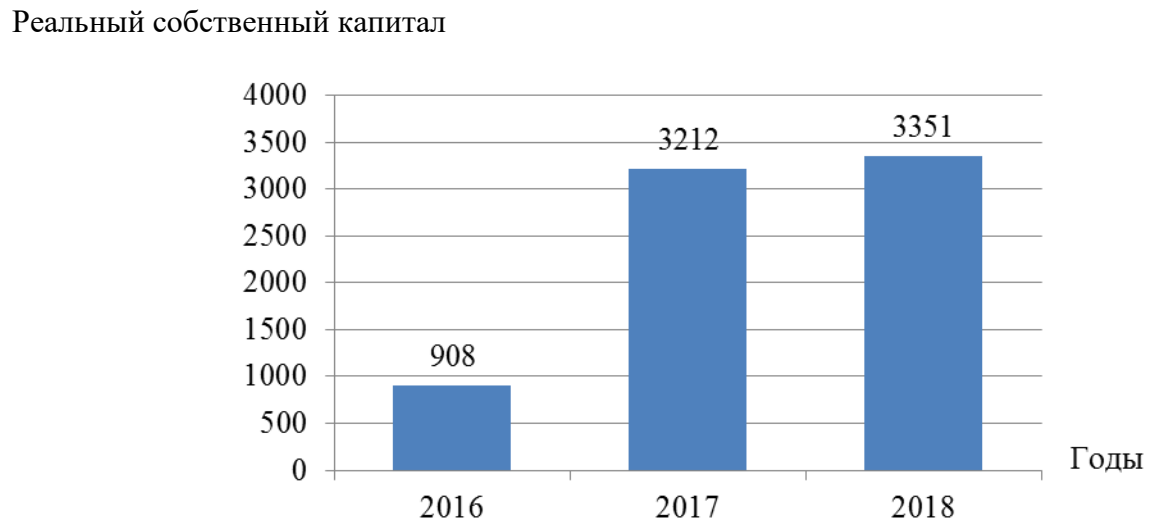


Рисунок 2.12 – Тенденция изменения реального собственного капитала ООО «ИнвестПрогрессЛогистик» за 2016-2018 гг.

Исходя из представленных данных, коэффициент автономии

за рассматриваемый период практически не изменил своего положения. Полученные значения за 2016-2018 гг. говорят о недостаточной доле

собственного капитала (6%) в общем капитале предприятия ООО «ИнвестПрогрессЛогистик».

Коэффициент обеспеченности собственными оборотными средствами составил на конец анализируемого периода (-0,24) при том, что по состоянию на 31.12.2017 г. коэффициент обеспеченности собственными оборотными средствами был намного меньше – (- 0,69)(произошел рост на 0,44). Стоит отметить, что полученные значения данного коэффициента являются не соответствующим принятому нормативу.

Коэффициент обеспеченности собственными оборотными средствами в течение всего периода не укладывался в установленный норматив(норматив составляет более 0,1).

За исследуемый период коэффициент покрытия инвестиций предприятия ООО «ИнвестПрогрессЛогистик» очень сильно увеличился на 0,23 и составил 0,3. Значение коэффициента на конец анализируемого периода не сосоответствует нормативу(доля собственного капитала ООО «ИнвестПрогрессЛогистик» и долгосрочных обязательств в общей сумме капитала организации составляет 30%). Нормативным значением данного показателя считается 1,5-2,5. Тенденция изменения коэффициента покрытия инвестиций представлена на рисунке 2.13.

Значение коэффициента покрытия инвестиций

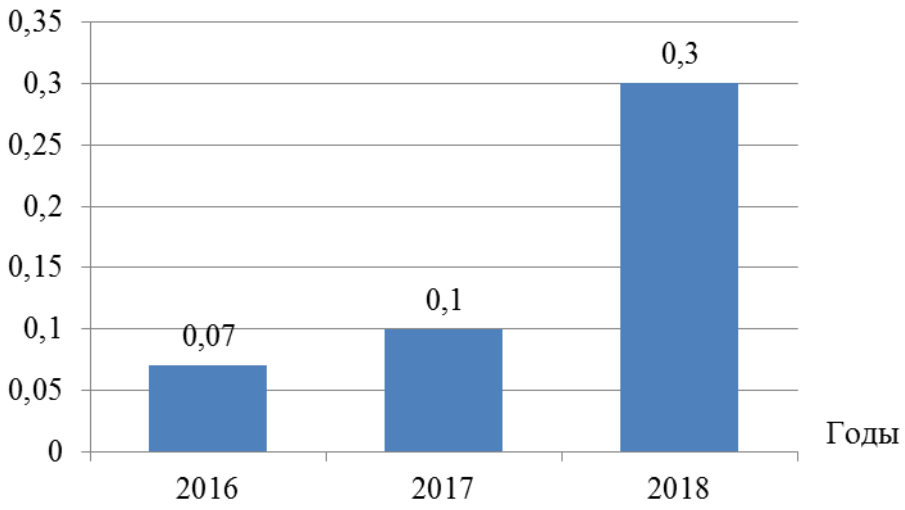


Рисунок 2.13 – Динамика коэффициента покрытия инвестиций ООО «ИнвестПрогрессЛогистик» за 2016-2018 гг.

Коэффициент обеспеченности материальными запасами за весь рассматриваемый период увеличился на 0,84, с (-1,59) до (-0,75). Данный показатель также в течение исследуемого периода не укладывался в установленный норматив, т.е. находится в области критических значений. На основании рассмотренных показателей стоит подчернкуть, что финансовое положение ООО «ИнвестПрогрессЛогистик» считается как неудовлетворительное. При этом, последние показатели покрытия собственными оборотными средствами запасов и затрат за 2016-2017 годы предприятия ухудшили свои значения.

Также частью оценки финансового анализа экономической безопасности предприятия транспортно-логистических услуг ООО «ИнвестПрогрессЛогистик» является определение показателей ликвидности. Ликвидность характеризуется подвижностью активов предприятия. Она предполагает возможность бесперебойной оплаты в срок кредитно-финансовых обязательств и законных денежных требований долга: наличность, депозиты в банке. Далее проведем анализ коэффициентов ликвидности предприятия, значения которого представлены в таблице 2.7.

Таблица 2.7 – Анализ коэффициентов ликвидности ООО «ИнвестПрогрессЛогистик»

Показатели	**Годы**		
	2016	**2017**	**2018**
Дебиторская задолженность	5 155,00	8 829,00	13 860,00
НДС по приобретенным ценностям	4 346,00	6 130,00	14 700,00
Общая сумма активов	17 031,00	33 038,00	53 043,00
Долгосрочные обязательства	333,00	628,00	12 427,00
Скорректированные краткосрочные обязательства	15 793,00	29 198,00	37 265,00
Коэффициент абсолютной ликвидности	0,001	0,20	0,32
Коэффициент критической ликвидности	0,33	0,50	0,69
Коэффициент покрытия (текущей ликвидности)	0,60	0,71	1,09
Коэффициент восстановления платежеспособности за 6 меясцев	-	0,38	0,64

В 2017 году коэффициент текущей (общей) ликвидности не укладывается в норму(нормативное значение равно 2). При этом за исследуемый период коэффициент текущей ликвидности вырос на 0,49 пункта. Отметим, что значение коэффициента быстрой ликвидности составило 0,69 в 2017 году. Это считается ниже нормативного значения. Данная ситуация говорит о том, что у предприятия ООО «ИнвестПрогрессЛогистик» недостаточно ликвидных активов (т. е. и других активов, которые можно легко обратить в наличность) для погашения краткосрочной кредиторской задолженности. Тенденция изменения краткосрочных обязательств предприятия «ИнвестПрогрессЛогистик» представлена на рисунке 2.14.

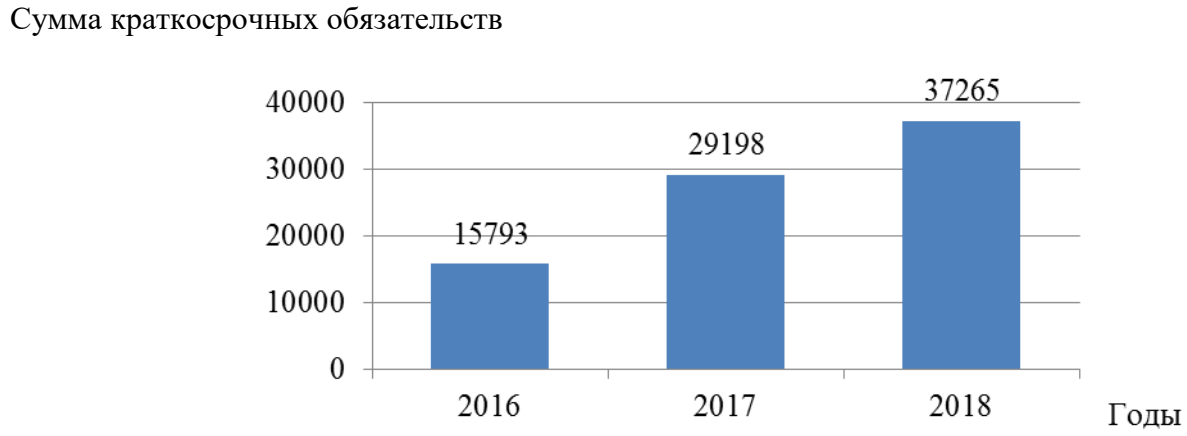


Рисунок 2.14 – Тенденция изменения краткосрочных обязательств предприятия ООО «ИнвестПрогрессЛогистик» за 2016-2018 гг.

Подчеркнем, что за 2016-2018 годы данный показатель сохранял значение, которое не соответствует норме. Третий показатель ликвидности – коэффициент абсолютной ликвидности, имеет значение, соответствующее норме в 2017 году (более 0,2). За два последних года коэффициент абсолютной ликвидности вырос на 0,319. Ликвидность активов – это способность активов трансформироваться в денежные средства. Ликвидность баланса предприятия – это уровень обеспеченности оборотных активов. Это предполагает изыскание платежных средств за счет внутренних источников,

т.е. реализации активов. Анализ соотношения активов по степени ликвидности и обязательств по сроку погашения приведен в таблице 2.8.

Таблица 2.8 – Анализ соотношения активов и пассивов в 2018 году

Активы по степени ликвидности	**На начало отчетного периода, тыс. руб.**	**Норм. соотношение**	**Пассивы по сроку погашения**	**На конец отчетного периода, тыс. руб.**	**Излишек/ недостаток платежных средств тыс. руб.**
А1	11896	≥	П1	37201	-25305
А2	13960	≥	П2	64	+13896
А3	13950	≥	П3	12427	+ 1523
А4	13237	≤	П4	3351	+9886

Из четырех соотношений, характеризующих соотношение активов по степени ликвидности и обязательств по сроку погашения, выполняется два. ООО «ИнвестПрогрессЛогистик» неспособно погасить наиболее срочные обязательства за счет высоколиквидных активов(денежных средств и краткосрочных финансовых вложений), которые составляют лишь 32% от достаточной величины. Далее рассмотрим показатели рентабельности, которые отражают эффективность, степень доходности предприятия. В таблице 2.9 представленные показатели рентабельности имеют положительные значения как следствие прибыльности деятельности ООО «ИнвестПрогрессЛогистик».

Таблица 2.9 – Оценка рентабельности «ИнвестПрогрессЛогистик» за 2017-2018 гг.

Показатели рентабельности	**Значения показателя (в %, или в копейках с рубля)**		**Изменение показателя**	
	2017 г.	**2018 г.**	**абс.**	**± %**
Рентабельность продаж по валовой прибыли	0,9	2,1	+1,2	+ 128,9

Рентабельность продаж по EBIT	4	0,8	-3,2	- 80,6
Рентабельность продаж по чистой прибыли	3	0,4	-2,6	-88
Прибыль от продаж на рубль, вложенный в реализацию услуг	0,9	2,1	+1,2	+131,7

Прибыль от продаж в анализируемом периоде составляет 2,1 % от полученной выручки. Более того, имеет место положительная динамика рентабельности обычных видов деятельности по сравнению с данным показателем (+ 128,9%).

Рентабельность, рассчитанная как отношение прибыли до налогообложения и процентных расходов(EBIT) к выручке организации, за 2017 год составила 0,8%. Это значит, что в каждом рубле выручки предприятия ООО «ИнвестПрогрессЛогистик» содержалось 0,7 коп. прибыли до налогообложения и процентов к уплате.

В итоге, в результате проанализируемой информации отмечено, что с негативной стороны финансовое положение предприятия и результаты деятельности организации характеризуют следующие показатели:

1) низкая величина собственного капитала относительно общей величины активов ООО «ИнвестПрогрессЛогистик» (6%);

2) ниже принятой нормы коэффициент текущей (общей) ликвидности;

3) не соответствует нормативному значению коэффициент быстрой(промежуточной) ликвидности; недостаточная рентабельность активов;

4) не соблюдается нормальное соотношение активов по степени ликвидности и обязательств по сроку погашения;

5) значительное падение прибыли до процентов к уплате и налогообложения (EBIT) на рубль выручки.

Анализируя экономическую безопасность предприятия, необходимо составить модель прогнозирования банкротства предприятия. Начнем с модели прогнозирования банкротства Р. Лиса, созданного для предприятий Великобритании в 1972 году. Это одна из первых европейских моделей, созданная после модели американца Э. Альтмана (1968). Модель Лиса

является в большей степени адаптационной, так как финансовые коэффициенты в модели взяты как у Альтмана. Формула модели банкротства Лиса представлена ниже:

$$Z=0,063\times K_1 + 0,092\times K_2 + 0,057\times K_3 + 0,001\times K_4, \quad (1)$$

где K_1 – рассчитывается как отношение оборотного капитала и активов;

K_2 – рассчитывается как отношение прибыли до налогообложения к активам предприятия;

K_3 – рассчитывается как нераспределенная прибыль к активам предприятия;

K_4 – рассчитывается как отношение собственного капитала к сумме долгосрочных и краткосрочных обязательств предприятия.

Сведем полученные результаты в следующую таблицу и оценим предприятие по методу банкротства. Отметим, что если $Z<0.037$– банкротство компании очень вероятно, если $Z>0.037$ – предприятие финансово устойчивое. Оценка вероятности банкротства по методике Лиса представлена в таблице 2.10.

Таблица 2.10 – Оценка вероятности банкротства по методике Лиса

Наименование показателя	**2016 г.**	**2017 г.**	**2018 г.**
Z-счет Лиса			
K_1	0,56	0,63	0,62
K_2	0,13	0,04	0,006
K_3	0,05	0,1	0,01
K_4	0,06	0,1	0,08
Значение коэффициента	0,05	0,05	0,05
	положение предприятия финансово устойчиво	положение предприятия финансово устойчиво	положение предприятия финансово устойчиво

Помимо модели Лиса для британских предприятий была построена модель Ричарда Таффлера. Для построения модели прогнозирования банкротства ученый взял 46 предприятий, которые обанкротились и 46

предприятий, которые остались финансово устойчивыми в период с 1969 по 1975 года. Ниже представлена формула расчета модели банкротства.

$$Z= 0,53\times K_1 + 0,13\times K_2 + 0,18\times K_3 + 0,16\times K_4 \quad (2)$$

где K_1 – соотношение прибыли от продаж к краткосрочным обязательствам;

K_2 – соотношение оборотных активов к сумме краткосрочных и долгосрочных обязательств;

K_3 – соотношение краткосрочных обязательств к активам;

K_4 – соотношение выручки к активам фирмы.

Рассмотрим условия оценки предприятия по модели банкротства Таффлера:

- если Z>-0,3 – предприятие маловероятно станет банкротом(« зеленая зона»),

- если Z<0,2 – предприятие вероятно станет банкротом («красная зона »),

- если 0,2<Z<0,3 – зона неопределенности(« серая зона») (таблица 2.11)

Таблица 2.11 – Оценка вероятности банкротства по методике Таффлера

Наименование показателя	**2016 г.**	**2017 г.**	**2018 г.**
Z-счет Таффлера			
K_1	0,09	0,01	0,02
K_2	0,6	0,7	0,7
K_3	0,93	0,9	0,7
K_4	1,83	1	0,7
Значение коэффициента	0,6	0,4	0,34
	«зеленая зона»: маловероятно станет банкротом	«зеленая зона»: маловероятно станет банкротом	«зеленая зона»: маловероятно станет банкротом

На основании методики Таффлера, за рассматриваемый период у предприятия прослеживается «зеленая зона», т.е. ООО «ИвестПрогрессЛогистик» маловероятно станет банкротом.

Следующая модель прогнозирования банкротства предприятия создана канадским ученым Гордоном Спрингейтом в университете Саймона Фрейзера. Половина коэффициентов совпадает с финансовыми коэффициентами, которые использовал Э. Альтман. Для создания модели оценки банкротства Спрингейт использовал финансовую отчетность от 40 предприятий Канады (20 банкротов / 20 небанкротов).

Формула модели банкротства Спрингейта представлена ниже:

$$Z= 1,03\times K_1 + 3,07\times K_2 + 0,66\times K_3 + 0,4\times K_4 \qquad (3)$$

Существует следующие условия:

- если $Z<0,862$ – банкротство предприятия вероятно;

- если – $Z>0,862$, банкротство предприятия маловероятно.

Далее представим оценку вероятности банкротства по методике Спрингейта в таблице 2.12.

Таблица 2.12 – Оценка вероятности банкротства по методике Спрингейта

Наименование показателя	**2016 г.**	**2017 г.**	**2018 г.**
Z-счет Спрингейта			
K_1	- 0,37	- 0,26	- 0,07
K_2	0,13	0,04	0,006
K_3	0,15	0,05	0,008
K_4	0,95	1	0,72
Значение коэффициента	0,5	0,3	0,3
	Банкротство предприятия вероятно	Банкротство предприятия вероятно	Банкротство предприятия вероятно

Среди критических показателей финансового положения организации можно выделить следующие: на конец 2017 года значение коэффициента обеспеченности собственными оборотными средствами (-0,25) можно охарактеризовать как явно не соответствующее принятому нормативу; крайне неустойчивое финансовое положение по величине собственных оборотных средств. Предприятию необходимо учитывать данные негативные факторы, иначе наступит ситуация банкротства.

На основании проведенного анализа, представим оценку интегрального уровня финансовой составляющей ООО «ИнвестПрогрессЛогистик» в таблице 2.13.

Таблица 2.13 – Оценка интегрального уровня финансовой составляющей фирмы

Показатели финансовой составляющей ЭБП	**Оценка (Оц) в зависимости от степени соответствия нормативу (в баллах)**			
	Обозначение	**2016 г**	**2017 г**	**2018 г**
Коэффициент автономии	Ка	0	0	0
Коэффициент обеспеченности собственными средствами	Ксос	0	0	0
Коэффициент абсолютной ликвидности	Кабл	0	0,5	1
Коэффициент текущей ликвидности	Ктл	0	0	0,5
Коэффициент быстрой ликвидности	Кб	0	0	0
Уровень финансовой составляющей	Уфс	0	0,1	0,3

Таким образом, на основании представленных данных(расчет показателей финансовой составляющей фирмы представлен в приложении Г) наблюдается низкий интегральный уровень финансовой составляющей экономической безопасности предприятия «Инвестпрогресслогистик».

В оценке интегрального уровня экономической безопасности предприятия также следует оценить производственно-сбытовую составляющую фирмы. Для этого используются значения коэффициентов:

- рентабельности продаж; рентабельности активов;
- соотношения дебиторской и кредиторской задолженности;
- оборачиваемости оборотных активов;
- уровня производственно-сбытовой составляющей (табл. 2.14).

Представим в таблице 2.14 оценку производственно-сбытовой составляющей ООО «ИнвестПрогрессЛогистик».

Таблица 2.14 – Оценка производственно-сбытовой составляющей фирмы

Показатели финансовой составляющей ЭБП	**Оценка (Оц) в зависимости от степени соответствия нормативу (в баллах)**			
	Обозначение	**2016 г**	**2017 г**	**2018 г**
Рентабельность продаж	Крп	1	1	1
Рентабельность активов	Кра	0	0	1
Коэффициент соотношения дебитор-ской и кредиторской	Ксдк	0	0	0

задолженностей				
Коэффициент оборачиваемости оборотных активов	Кооб	0,5	0	0,5
Уровень производственно-сбытовой составляющей	Упсс	0,38	0,25	0,63

На основании представленных данных наблюдается положительное значение в 2017 году: уровень производственно-сбытовой составляющей составил 0,63. Наблюдается положительная динамика рентабельности продаж. Далее проведем оценку технико-технологической составляющей экономической безопасности фирмы в таблице 2.15.

Таблица 2.15 – Оценка технико-технологической безопасности предприятия

Показатели финансовой составляющей ЭБП	**Оценка (Оц) в зависимости от степени соответствия нормативу (в баллах)**			
	Обозначение	**2016 г**	**2017 г**	**2018 г**
Обновления основных средств	Коб.	1	0,5	1
Фондоотдачи	Кф	1	1	1
Годности основных средств	Кг	0,5	0,5	0,5
Уровень технико-технологической составляющей	Упсс	0,8	0,7	0,8

В целом, ситуацию по оценке технико-технологической безопасности предприятия можно назвать положительной.

Далее проведем оценку кадровой составляющей экономической безопасности предприятия ООО «ИнвестПрогрессЛогистик». Для этого необходимо рассмотреть такие составляющие, как: коэффициент уровня заработной платы; показатель стабильности кадров; коэффициент выработки на одного сотрудника. Оценка кадровой составляющей представлена в таблице 2.16.

Таблица 2.16 – Оценка кадровой составляющей фирмы

Показатель/составляющая экономической безопасности	**Оценка (Оц) в зависимости от степени соответствия нормативу (в баллах)**			
	Ошибка	**Ошибка (оценка 1)**	**Нейтральное(оценка 0,5)**	**Критическое (оценка 0)**
Коэффициент уровня з/п	Кзп	>1	0,5-1	<0,5

Показатель стабильности кадров	Кск	>1	0,5-1	<0,5
Коэффициент выработки продукции на одного сотрудника	Квыр	Рост **Ошибка**	Значение показателя практически не меняется	Снижение показателя в динамике
Уровень кадровой составляющей		Укс = 0,5 + 0 + 0,5 = 0,33		

На основании проведенной оценки составляющих уровня экономической безопасности сведем полученные значения в таблицу 2.17.

Таблица 2.17 – Результаты сводной оценки интегрального уровня экономической безопасности фирмы

Составляющие экономической безопасности предприятия	**Оценка (Оц) в зависимости от степени соответствия нормативу (в баллах)**			
	Обозначение	**2016**	**2017**	**2018**
Финансовая	Уфс	0	0,1	0,3
Производственно-сбытовая	Упсс	0,38	0,25	0,63
Кадровая	Укс	0,5	1	0,33
Технико-технологическая	Уттс	0,8	0,7	0,8
Сводный интегральный уровень экономической безопасности фирмы	ИУэб	0,42	0,51	0,52

На основании представленных данных в последний год наблюдается незначительное повышение интегрального уровня экономической безопасности предприятия: технико-технологическая составляющая уменьшилась в 2018 году по сравнению с предыдущим годом на 0,1; кадровая составляющая в 2018 году на 0,67. Финансовая составляющая увеличилась на 0,2 норматива, однако характеризуется неудовлетворительной ситуацией в осуществлении предпринимательской деятельности фирмы.

Таким образом, в данном параграфе была проведена оценка интегрального уровня экономической безопасности предприятия, где выяснилось, что уровень экономической безопасности фирмы следует увеличивать за счет финансовой составляющей и кадровой.

2.3. Оценка системы защиты информации на предприятии

На сегодняшний день транспорт – одна из важнейших отраслей хозяйства, обеспечивающая потребности населения в перевозках. Специфика

транспорта как сферы экономики заключается в том, что он сам не производит новой продукции, а только участвует в ее создании, обеспечивая сырьем, материалами, оборудованием производство и, доставляя готовую продукцию потребителю, увеличивая тем самым её стоимость на величину транспортных издержек, которые включаются в себестоимость.

По некоторым отраслям промышленности транспортные издержки очень значительны, как, к примеру, в лесной промышленности, где они могут достигать 50%. Полные же транспортные издержки в сфере производства и обращения составляют 10% от валового общественного продукта страны. Отношение суммарных транспортных издержек к полной стоимости продукта у потребителя называют коэффициентом транспортной слагающей. Транспортный фактор имеет немаловажное значение на нашем региональном рынке, с его географическим положением, ресурсами, населением и основными производственными фондами.

В условиях перехода к рыночным отношениям роль транспорта существенно возрастает, что говорит о том, что постоянно необходимо совершенствовать транспортные технологии. С одной стороны, от транспортного фактора зависит эффективность работы фирмы, что в условиях рынка напрямую связано с его жизнеспособностью, а, с другой стороны, сам рынок подразумевает обмен товарами и услугами, что без транспорта невозможно, а, следовательно, невозможен и сам рынок. Поэтому транспорт является важнейшей составной частью рыночной инфраструктуры. Важной особенностью транспортной системы является её тесная взаимосвязь с производством. Инновационный путь расширенного производства в Белгородском регионе ставит перед транспортом ряд важных проблем, требующих неотложного решения:

1) комплексное развитие транспортной системы ппредприятия « ИнвестПрогрессЛогистик»;

2) применение инновационной техники для погрузочно-разгрузочных работ;

3) совершенствование структуры автомобильного транспорта (по типу кузова и грузоподъемности);

4) подготовка и повышение квалификации работников, занятых не только эксплуатацией новой техники, но и техническим обслуживанием, и текущим ремонтом;

5) совершенствование организации производства и труда;

6) сокращение внутрисменных простоев транспортных средств, потерь сырья и топлива, рабочего времени.

Поэтому вопросам обеспечения информационной безопасности уделяется все больше внимания. Результаты оценки информационных активов сведены в таблицу 2.18.

Таблица 2.18 – Оценка информационных активов предприятия

Вид деятельности	**Ошибка! актива**	**Форма представления**	**Владелец актива**	**Критерии определения стоимости**	**Размерность оценки**
					Качественная
Информационные активы					
1. **Ошибка!** деятельность	Отчеты о деятельность подразделений	Электронная	директор	Ущерб от потери **Ошибка! Ошибка!**	очень высокая
2. Все виды деятельности	Сервер БД электронных писем	Электронная	директор	Ущерб от потери **Ошибка!** в электронной почте	очень высокая
3. Основная деятельность	Сервер БД с информацией о клиентах	Бумажный и электронный документ	Финансовый директор	**Ошибка!** стоимость	очень высокая
4. Работа с персоналом	Договора, контракты	Бумажный и электронный документ	Отдел кадров	Первоначальная стоимость	высокая
5.Общее руководство администрацией и оперативно-хозяйственной деятельностью предприятия	Приказы, распоряжения	Бумажный и электронный документ	Генеральный директор	**Ошибка!** стоимость	очень высокая
6. Бухгалтерский учет	База данных бухгалтерии	1С предприятие	Финансовый директор	**Ошибка!** стоимость	Очень высокая

К объектам защиты относят, как правило, системы для комплексного учета, планирования и управления бизнес-процессами, в том числе управления перевозками, автоматизированные системы управления жизнеобеспечения транспортными объектами, системы обеспечения безопасности и информационно-телекоммуникационные сети.

Следует отметить, что на исследуемом предприятии отсутствует отдел по информационной безопасности – что является существенным недостатком в работе предприятия. Необходимо принять во внимание все, что может пострадать от нарушений режима безопасности. Может быть использована следующая классификация активов:

- аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, мосты, маршрутизаторы;
- программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы.

В таблице 2.19 представим оценку физических активов фирмы ООО «ИнвестПрогрессЛогистик».

Таблица 2.19 – Оценка физических активов предприятия

Вид деятельности	**Ошибка! актива**	**Форма представления**	**Владелец актива**	**Критерии Ошибка! стоимости**	**Размерность оценки**
					Качественная
Физические активы					
1.Все виды деятельности	Сервер с базой электронных писем	Электронная	Генеральный директор	Ущерб от потери информации в **Ошибка!** почте	очень высокая
2. Основная деятельность	Здания сооружения, материалы	Здания, сооружения, транспортные средства, материалы	Зам.генерального директора	Основные средства	Высокая
3.Заключение договоров на оказание услуг	Договора, контракты	Бумажный и электронный документ	Генеральный директор, финансовый директор	Конечная стоимость	Высокая

Результаты ранжирования активов представлены в таблице 2.20.

Таблица 2.20 – Результаты ранжирования активов ООО «ИнвестПрогрессЛогистик»

Наименование актива	**Ценность актива(ранг)**
Сервер БД с информацией о клиентах	1
Сервер с базой электронных писем;	1
База данных ДО	1
Приказы, распоряжения директора	1
База данных бухгалтерии	1
Отчеты о деятельность подразделений	2
Договора, контракты	2
Работа с персоналом	3
Здания сооружения, материалы, транспорт	4

Таким образом, активы, имеющие наибольшую ценность и подлежащие защите, следующие:

1. Сервер БД с информацией о клиентах и писем;
2. База данных ДО;
3. Приказы, распоряжения директора;
4. База данных бухгалтерии.

В дальнейшем именно для этих активов следует проводить оценку уязвимостей, угроз и рисков информационной безопасности. В качестве объектов защиты выступают следующие виды информационных ресурсов предприятия:

- информация (данные, телефонные переговоры и факсы) передаваемая по каналам связи;
- информация, хранимая в базах данных, на файловых серверах и рабочих станциях, на серверах каталогов, в почтовых ящиках пользователей корпоративной сети и т.п.;
- конфигурационная информация и протоколы работы сетевых устройств, программных систем и комплексов;
- информация о маршруте транспортных средств.

В таблице 2.21 представлено сопоставление физических угроз и уязвимости активов.

Таблица 2.21 – Сопоставление физических угроз и уязвимостей фирмы

УГРОЗЫ АРМ	**УЯЗВИМОСТИ АРМ**
1) Физический доступ нарушителя к АРМ	1) Отсутствие системы контроля доступа сотрудников к чужим АРМ
	2) Отсутствие системы видеонаблюдения в организации
	3) Несогласованность в системе охраны периметра
2) Разглашение конфиденциальной информации, хранящейся на рабочем месте сотрудника организации	1) Отсутствия соглашения о неразглашении между работником и работодателем
	2) Нечеткая регламентация ответственности сотрудников организации
2. УГРОЗЫ СЕРВЕРОВ	2. УЯЗВИМОСТИ СЕРВЕРОВ
1) Физический неавторизованный доступ нарушителя в серверную комнату	1) Неорганизованный контрольно-пропускной режим в организации
	2) Отсутствие видеонаблюдения в серверной комнате
	3) Отсутствие охранной сигнализации
2) Разглашение конфиденциальной информации	1) Отсутствие соглашения о нераспространении конфиденциальной информации
	2) Нечеткая регламентация ответственности сотрудников организации
3. УГРОЗЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ	3. УЯЗВИМОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
1). Физический доступ нарушителя к носителям с конфиденциальной информации	1) Неорганизованность контрольно-пропускного пункта
	2) Отсутствие системы видеонаблюдения в организации
	3) Отсутствие системы охранной сигнализации
2). Разглашение конфиденциальной информации, в документах, вынос носителей за пределы контролируемой зоны	1) Отсутствие соглашения о неразглашении конфиденциальной информации
	2) Нечеткое распределение ответственности за документы(носители конфиденциальной информации) между сотрудниками организации
3).Несанкционированное копирование, печать и размножение носителей конфиденциальной информации	1) Нечеткая организация конфиденциального документооборота в организации
	2) Неконтролируемый доступ сотрудников к копировальной и множительной технике
4. Угрозы сетевых устройств и коммутационного оборудования	4. Уязвимости сетевых устройств и коммутационного оборудования
1). Физический доступ к сетевому устройству	1) Неорганизованный контрольно-пропускной режим в организации
	2) Отсутствие системы видеонаблюдения в организации
	3) Несогласованность в системе охраны периметра
	4) Нечеткая регламентация ответственности сотрудников предприятия
2). Разрушение (повреждение, утрата) сетевых устройств и коммутационного оборудования	1) Отсутствие ограничения доступа к сетевым устройствам и коммутационному оборудованию, внутренней сети предприятия
	2) Нечеткая регламентация ответственности сотрудников предприятия

Результаты оценки уязвимости информационных активов представлены в приложении Д.

Рассмотрим перечень возможных угроз для информации и активов в таблице 2.22.

Таблица 2.22 – Возможные угрозы для информации и активов

Группа угроз Содержание угроз	**Отчеты о деятельности подразделений**	**Сервер с базой электронных писем**	**База данных бухгалтерии**	**Сервер БД с информацией о клиентах**
1. Угрозы, обусловленные преднамеренными действиями				
Намеренное повреждение	Высокое	Высокое	Высокое	Высокое
Кража	Высокое	Средняя	Средняя	Средняя
Несанкционированное использование носителей данных	Высокое	Высокое	Высокое	Высокое
Использование несанкционированного доступа	Высокое	Высокое	Высокое	Высокое
Вредоносное программное обеспечение	Высокое	Средняя	Средняя	Средняя
Повреждение линий	Низкая	Низкая	Низкая	Низкая
2. Угрозы, обусловленные случайными действиями				
Пожар	Средняя	Средняя	Средняя	Средняя
Затопление	Низкая	Низкая	Низкая	Низкая
Неисправность в электроснабжении.	Средняя	Высокое	Высокое	Высокое
Неисправность в водоснабжении.	Низкая	Низкая	Низкая	Низкая
Неисправность в системе кондиционирования воздуха.	Средняя	Средняя	Средняя	Средняя
Колебания напряжения.	Высокое	Высокое	Высокое	Высокое
Аппаратные отказы.	Высокое	Высокое	Высокое	Высокое
Экстремальные величины температуры и влажности	Низкая	Низкая	Низкая	Низкая
Воздействие пыли	Низкая	Низкая	Низкая	Низкая
Ошибки обслуживающего персонала	Низкая	Низкая	Низкая	Низкая
Программный сбои	Высокое	Высокое	Высокое	Высокое
3. Угрозы, обусловленные естественными причинами (природные, техногенные факторы)				
Землетрясение	Низкая	Низкая	Низкая	Низкая
Ураган	Низкая	Низкая	Низкая	Низкая
Попадание молнии	Низкая	Низкая	Низкая	Низкая

Информационная безопасность ООО «ИнвестПрогрессЛогистик» - состояние защищенности информационных ресурсов в вычислительных сетях и системах предприятия от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальное функционирование систем, попыток разрушения её компонентов.

Цели защиты информации ООО «ИнвестПрогрессЛогистик»

- предотвращение угроз безопасности предприятия вследствие несанкционированных действий по уничтожению, модификации, искажению,

копированию, блокированию информации или иных форм незаконного вмешательства в информационные ресурсы и информационных системах;

- сохранение коммерческой тайны, обрабатываемой с использованием средств вычислительной техники;

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах.

Представим количественный анализ рисков информационной безопасности. Рассмотрим методику на примере веб-сервера организации, который используется для продажи определенного товара. Количественный разовый ущерб от выхода сервера из строя можно оценить как произведение среднего чека покупки на среднее число обращений за определенный временной интервал, равное времени простоя сервера. Допустим, стоимость разового ущерба от прямого выхода сервера из строя составит 100 тысяч рублей.

Теперь следует оценить экспертным путем, как часто может возникать такая ситуация (с учетом интенсивности эксплуатации, качества электропитания и т.д.). Например, с учетом мнения экспертов и статистической информации, мы понимаем, что сервер может выходить из строя до 2 раз в год.

Умножаем две эти величины, получаем, что среднегодовой ущерб от реализации угрозы прямого выхода сервера из строя составляет 200 тысяч рублей в год.

Эти расчеты можно использовать при обосновании выбора защитных мер. Например, внедрение системы бесперебойного питания и системы резервного копирования общей стоимостью 100 тысяч рублей в год позволит минимизировать риск выхода сервера из строя и будет вполне эффективным решением.

Для решения угроз фирмы следует открыть вакансию – специалист по информационной безопасности; закупить программное обеспечение для

решения вопросов по информационной безопасности.

Отметим, что для каждого объекта распределительной информационной системы(РИС) в базе данных имеется 3 таблицы:

- таблица сведений о событиях, в которую внесена информация, собранная в результате мониторинга ООО «ИнвестПрогрессЛогистик»;

- таблица контрольных значений, с которыми в процессе аудита сравниваются значения из таблиц первой группы;

- таблица событий, идентифицированных как атаки на РИС, в которой содержится информация, полученная в результате аудита событий из первой таблицы.

Оцениваемый компонент РИС – хост 1, подключенный к серверу 1. На данный хост могут оказывать воздействие инсайдер и внешний злоумышленник (2 категории злоумышленников). Со стороны злоумышленника первой категории могут оказывать воздействие следующие атаки:

- атака 1 «несанкционированный вход в систему» посредством подбора пароля входа в систему;

- атака 2 «несанкционированный доступ к объектам»;

- атака 3 «несанкционированная загрузка системы».

Представим расчет риска информационной безопасности (возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации) на основе модели угроз и уязвимостей предприятия. Рассмотрим расчет рисков для одной угрозы информационной безопасности, т.к. для остальных угроз риск рассчитывается аналогично в таблице 2.23.

Таблица 2.23 – Исходные данные по угрозам и уязвимости предприятия

Ресурс фирмы	**Угрозы фирмы**	**Уязвимости фирмы**
Сервер	Угроза 1 характеризуется неавторизованным проникновением нарушителя внутрь охраняемого периметра(одного из периметров)	Уязвимость 1 Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию
		Уязвимость 2 Отсутствие системы наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом(или существующая система наблюдения охватывает не все важные объекты)
	Угроза 2 характеризуется неавторизованной модификацией информации в системе электронной почты, хранящейся на ресурсе	Уязвимость 1 Отсутствие авторизации для внесения изменений в систему электронной почты
		Уязвимость 2 Отсутствие регламента работы с системой криптографической защиты электронной корреспонденции
	Угроза 3 характеризуется разглашением конфиденциальной информации сотрудниками предприятия	Уязвимость 1 Отсутствие соглашений о конфиденциальности
		Уязвимость 2 Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками

Представим процентное значение вероятности реализации угрозы через уязвимость в 2018 году, а также критичность реализации угрозы через уязвимость на основании оперативных данных фирмы в следующей таблице 2.24.

Таблица 2.24 – Данные предприятия для оценки уровня информационной угрозы

Угроза/уязвимость	**Вероятность реализации угрозы через уязвимость в течение 2018 года (%), P(V)**	**Критичность реализации угрозы через уязвимость (%), ER**
Угроза 1 / Уязвимость 1	40	50
Угроза 1 / Уязвимость 2	10	50
Угроза 2 / Уязвимость 1	50	30
Угроза 2 / Уязвимость 2	5	35
Угроза 3 / Уязвимость 1	5	75
Угроза 3 / Уязвимость 2	70	70

На основании представленных данных наблюдается наибольшая вероятность реализации угрозы (70%) через уязвимость в течение 2018 года, которая характеризуется разглашением конфиденциальной информации сотрудниками предприятия, а точнее распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками. Угроза 2 (50%) характеризуется неавторизованной модификацией информации в системе электронной почты, хранящейся на ресурсе, здесь прослеживается отсутствие авторизации для внесения изменений в систему электронной почты. Далее проведем расчет уровня информационных угроз «ИнвестПрогрессЛогистик» в таблице 2.25.

Таблица 2.25 – Оценка уровней информационных угроз ООО «ИнвестПрогрессЛогистик»

Угроза/уязвимость	**Уровень угрозы (%), Th** **Th = (ER/100) × (P(V)/100)**	**Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh** **CTh = 1 – П (1- CTh)**
Угроза 1 / Уязвимость 1	0,2	0,24
Угроза 1 / Уязвимость 2	0,05	
Угроза 2 / Уязвимость 1	0,02	0,04
Угроза 2 / Уязвимость 2	0,02	
Угроза 3 / Уязвимость 1	0,04	0,51
Угроза 3 / Уязвимость 2	0,49	

И на основании оценки уровней информационных угроз ООО «ИнвестПрогрессЛогистик» представим оценку общего уровня информационных угроз в таблице 2.26.

Таблица 2.26 – Оценка общего уровня информационных угроз фирмы

Угроза/уязвимость	**Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh** **CTh = 1 – П (1- CTh)**	**Общий уровень угроз по ресурсу(%) CThR**
Угроза 1 / Уязвимость 1	0,24	0,6424
Угроза 1 / Уязвимость 2		
Угроза 2 / Уязвимость 1	0,04	
Угроза 2 / Уязвимость 2		
Угроза 3 / Уязвимость 1	0,51	
Угроза 3 / Уязвимость 2		

Согласно полученному значению, наблюдается следующее: по значениям в представленной матрице прогнозируется высокая вероятность атак и высокая вероятность ущерба. Рассмотрим матрицу рисков в таблице 2.27.

Таблица 2.27 – Матрица рисков (согласно рекомендациям NIST «Risk Management Guide for Information Technology Systems»)

Вероятность атаки (P)	**Ущерб**		
	Низкий 0 < У < = 10 (%)	**Средний 10 < У < = 50 (%)**	**Высокий 50 < У < = 100 (%)**
Высокая (0,5 < P < = 1)	Низкий 5 < R < = 10 (%)	Средний 10 < R < = 50 (%)	Высокий 50 < У < = 100 (%)
Средняя (0,1 < P < = 0,5)	Низкий 1 < R < = 5 (%)	Средний 5 < R < = 25(%)	Высокий 50 < R < = 100 (%)
Низкая (0 < P < = 0,1)	Низкий 0 < R < = 1 (%)	Низкий 0 < R < = 5 (%	Низкий 0 < R < = 10 (%)

Следовательно, система не защищена и необходимо принять меры по снижению остаточного риска до приемлемого уровня и по усилению защиты информационной системы. Также хотелось отметить вторую угрозу информационной безопасности, но уже стороны сотрудников, которые осуществляют перевозку грузов. В рамках прохождения преддипломной практики было выяснено следующее: в последнее время на предприятие поступает недостоверная информация сотрудников по следующим показателям

По данным фирмы затраты засчет недоставерной информации составляли в прошлом году около 822 000 рублей, а в 2018 году – 1 088 000 рублей.

Представим результаты сводной оценки интегрального уровня экономической безопасности предприятия с учетом информационной составляющей в следующей таблице 2.28.

Таблица 2.28 – Результаты сводной оценки интегрального уровня экономической безопасности фирмы с учетом информационной составляющей

Составляющие экономической безопасности предприятия	Оценка (Оц) в зависимости от степени соответствия нормативу	
	Обозначение	2018
Финансовая	Уфс	0,3
Производственно-сбытовая	Упсс	0,63
Кадровая	Укс	0,33
Технико-технологическая	Уттс	0,8
Информационная	Уиб	0,36
Сводный интегральный уровень ЭБП	ИУэб	0,47

Иллюстративно представим виды недоставерной информации на рисунке 2.15.

Рисунок 2.15 – Виды недоставерной информации, предоставляемые сотрудниками фирмы «ИнвестПрогрессЛогистик»

Таким образом, сводный интегральный уровень экономической безопасности фирмы находится на средней позиции и составляет 0,47. Подчеркнем, что информационная безопасность предприятия – это не только предотвращение

« утечек» информации, но и создание условий для ее контроля на наличие достоверности и четкости. В следующей главе представим мероприятия по повышению уровня информационной безопасности.

ГЛАВА 3. РАЗРАБОТКА ПРОЕКТА ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

3.1. Общая характеристика предлагаемого проекта

На сегодняшний день экономическую безопасность предпринимательской деятельности можно определить как «защищенность жизненно важных интересов коммерческого предприятия от внутренних и внешних угроз, защиту кадрового и интеллектуального потенциала, технологий, данных и информации, капитала и прибыли, которая обеспечивается системой мер правового, экономического, организационного, информационного, инженерно-технического и социального характера. Представим место информационной безопасности в общей системе безопасности предприятия на рисунке 3.1.

Рисунок 3.1 – Место информационной безопасности в системе безопасности ООО «ИнвестПрогрессЛогистик»

На основании необходимости достижения целей обеспечения экономической безопасности предпринимательской деятельности компании« ИнвестПрогрессЛогистик», необходимо определить основные проблемные направления:

- организацию эффективной защиты материальной, финансовой и интеллектуальной собственности;
- защиту информационных ресурсов предприятия;
- эффективное управление ресурсами и персоналом.

Информационная безопасность фирмы – это состояние защищен-ности информационной среды предприятия, обеспечивающее его функцио-нирование и развитие в интересах его персонала.

На сегодняшний день в области недобросовестной конкуренции выработаны разнообразные методы и приемы получения информации об оказываемых услугах, о приемах их оказывания. Также большой угрозой для организации выступает персонал. Основная проблема обеспечения информационной безопасности состоит в большой роли человеческого фактора. В случае отсутствия четкого мониторинга, сотрудники могут «сливать» информацию о деятельности фирмы, осуществлять хищение.

За последние два года затраты фирмы были увеличены. На предприятии отсутствует четкая информационная система контроля за работой сотрудников. Отсутствует четкая информация по следующим аспектам:

- анализ расхода горюче-смазочных материалов;
- контроль режима труда и отдыха;
- контроль своевременного обслуживания оборудования;
- контроль реального пробега;
- время простоя; отчеты по поездкам и хронологии движения;
- отчет по моточасам для анализа продуктивности движения;
- планирование и контроль соблюдения маршрута;
- контроль качества оказываемых услуг; сводная отчетность по выполнению заявок.

Информационная безопасность предприятия – это не только предотвращение «утечек» информации, но и создание условий для ее контроля на наличие достоверности и четкости. В целях решения указанных выше проблем, ООО «ИнвестПрогрессЛогистик» предлагается приобрести программный продукт по информационной безопасности – Wialon.

Wialon – программная платформа с web-интерфей-сом для спутникового мониторинга транспорта. Система обладает рядом функций,

присущих программному обеспечению для мониторинга и управления автопарками.

Wialon разрабатывается белорусской компанией Gurtam. Впервые в России Wialon был представлен на выставке Навитех-Экспо 2009. В 2010 году Wialon был впервые продемонстрирован зарубежной аудитории на выставке CeBIT 2010. Gurtam была единственной компанией-разработчиком ПО из Белоруссии. В этом же году на выставке Навитех-экспо 2010 была представлена новая версия системы мониторинга транспорта Wialon. Представим особенности системы мониторинга на рисунке 3.2.

Рисунок 3.2 – Основные особенности системы мониторинга Wialon

Система мониторинга Wialon позволяет получать дополнительную прибыль и снижать риск порчи и хищения груза, обеспечивая контроль автопарка в реальном времени. Подчеркнем, что полноценное обеспечение информационной безопасности ООО «ИнвестПрогресс-Логистик» реально только при правильном подходе к защите данных. В системе

информационной безопасности нужно учитывать все актуальные на сегодняшний день угрозы и уязвимости. Представим иллюстративно возможности система мониторинга Wialon на рисунке 3.3.

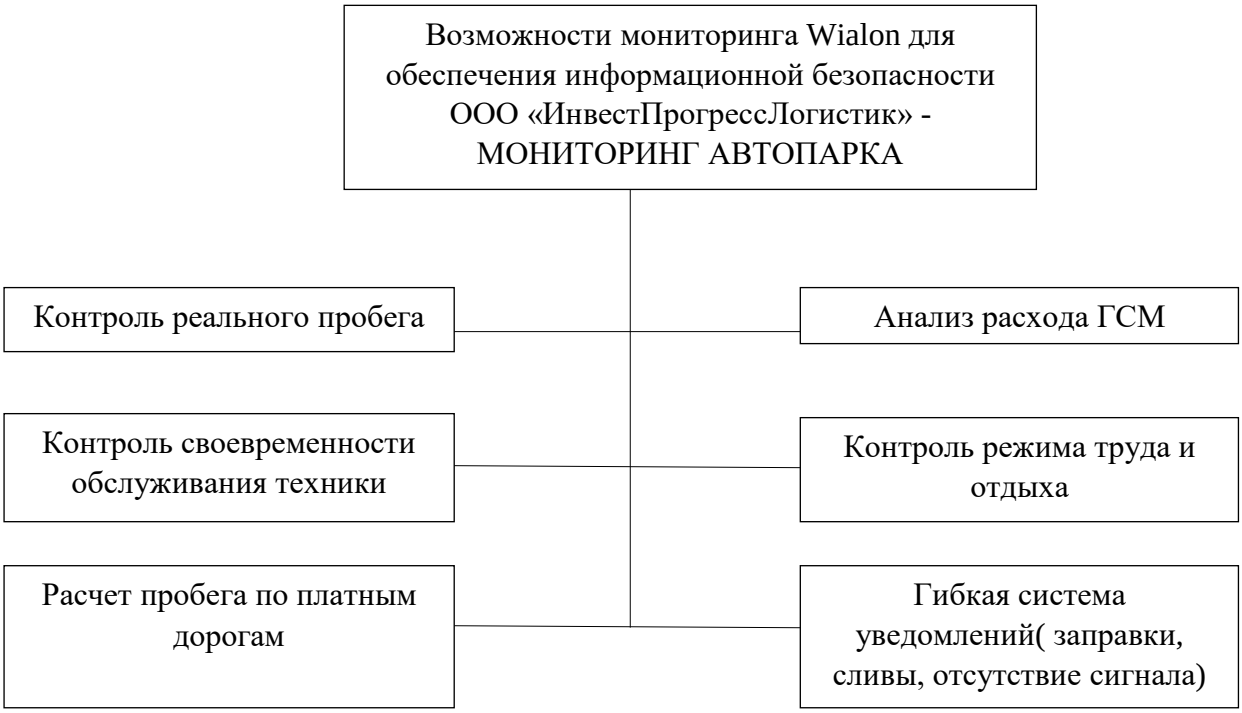


Рисунок 3.3 – Возможности мониторинга Wialon для обеспечения информационной – мониторинг автопарка

Подчеркнем, что контроль грузоперевозок и постоянное отслеживание груза обеспечивают точное соблюдение сроков и условий доставки, повышая уровень удовлетворенности клиентов и поддерживая стабильно высокий имидж компании, сохраняя стабильность информационной безопасности.

Отметим, что Wialon обеспечивает контроль эксплуатации техники и оборудования, предотвращая повышенный износ и критические поломки. Благодаря системе отчетов и уведомлений фирма будет обеспечена определенной информацией, где, когда и насколько эффективно используется техника ООО «ИнвестПрогрессЛогистик», и сможет на «корню » предотвратить любые попытки саботировать рабочий процесс.

Непосредственно, необходимо отметить универсальность данной системы: Wialon позволяет обеспечить информационную безопасность за счет контроля эксплуатации онлайн:

- мониторинг учитывает время полезной работы и простоя;
- учитывает работу двигателя под нагрузкой для мониторинга длительности и эффективности работы навесного оборудования;
- контролирует обороты двигателя.

При этом система контролирует процесс технического обслуживания:

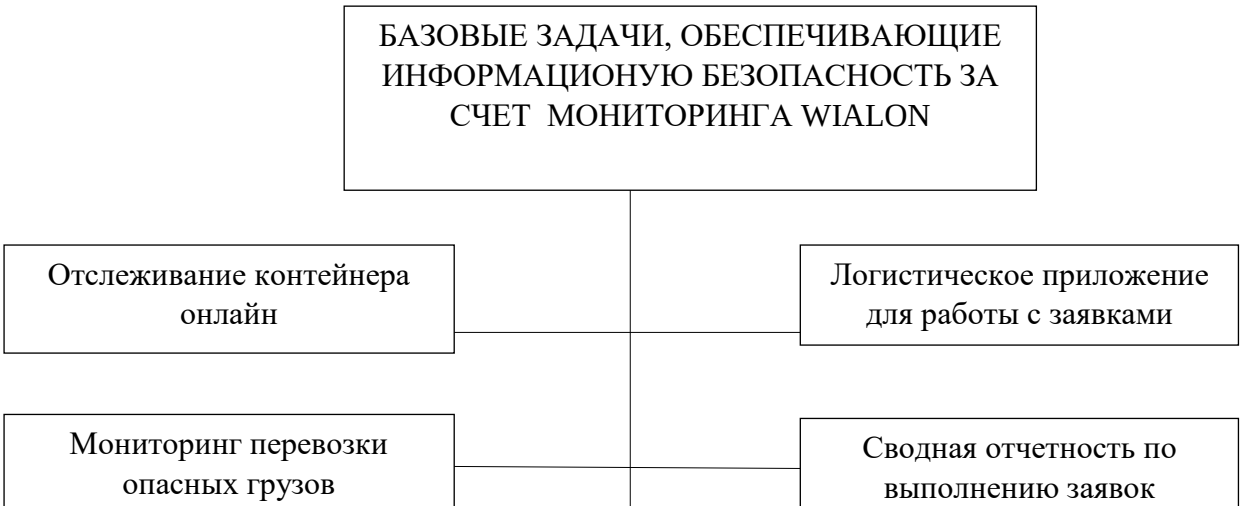
- уведомляет о предстоящем или просроченном техническом обслуживании;
- ведет журнал техобслуживания.

Проводит аналитику:

- отчетность по прохождению технического обслуживания;
- регистрация событий для последующих отчетов;
- отчеты по поездкам и хронологии движения;
- отчет по моточасам для анализа продуктивности движения.

Система мониторинга обеспечивает контроль грузоперевозок и постоянно осуществляет отслеживание груза, при этом соблюдаются сроки и условия доставки, повышая уровень удовлетворенности клиентов и поддерживая стабильно высокий имидж компании« ИнвестПрогрессЛогистик».

Данный проект по информационной безопасности обеспечивает решение следующих задач, представленных иллюстративно на рисунке 3.4.



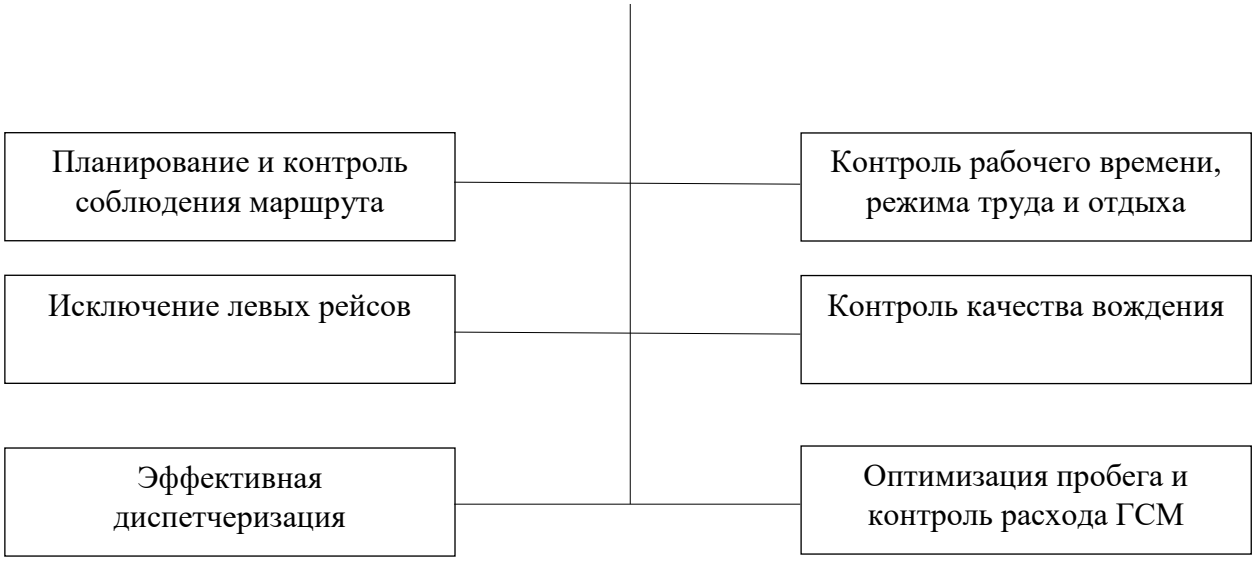


Рисунок 3.4 – Базовые задачи, обеспечивающая информационная безопасность за счет мониторинга Wialon

На основании представленных базовых задач, которые обеспечивает информационная безопасность за счет мониторинга Wialon, система предлагает больше, чем просто отображение объектов на карте: формируется объективная информация об активности и состоянии объекта в реальном времени и оперативно фирма может реагировать на тревожные события.

Дополнительные возможности мониторинга Wialon:

- контроль скорости по дорожным или кастомным ограничениям;
- привязка видео с web-камер к геозоне;
- определение местоположения по базовым станциям мобильных операторов;
- быстрые отчеты по объекту;
- отправка команд из панели мониторинга.

Wialon упростит работу с маршрутами благодаря автоматическому планированию и оптимизации. С данной системой возможно прохождение

маршрута в реальном времени, оперативно реагируя на отклонения и несанкционированные остановки. Также можно использовать данные для анализа и совершенствования логистики ООО «ИнвестПрогрессЛогистик».

Аналитика Wialon:

- история маршрута с данными по опозданиям и опережениям;
- отчетность по рейсам для объекта и маршрута;
- построение и трассировка треков;
- расчет пробега по платным дорогам;
- отчет по выполненным заявкам;
- треки, маркеры и геозоны в отчетах.

За счет системы Wialon осуществляется контроль в реальном времени:

- контроль прохождения маршрутов и посещения контрольных точек посредством геозон;
- уведомления при прохождении маршрута, опоздании или отклонениях.

Системы Wialon позволяет контролировать условия транспортировки:

- контроль температуры;
- контроль открытия/закрытия дверей;
- контроль веса и нагрузки на ось;
- контроль включения/выключения рефрижератора;
- контроль зажигания.

Спутниковая поисково-охранная система сводит риск потери авто к минимуму. В случае угона, потери груза или нарушения договора лизинга противоугонная система поможет установить точное местоположение объекта и отслеживать его в режиме онлайн вплоть до обнаружения. С решениями Wialon возможно обеспечивать безопасность корпоративных автомобилей 24/7. Система по обеспечению информационной безопасности предприятия «ИнвестПрогрессЛогистик» позволяет осуществлять мониторинг активности сотрудников, который представлен на рисунке 3.5.

Мониторинг активности сотрудников как фактор обеспечения информационной безопасности ООО «ИнвестПрогрессЛогистик»

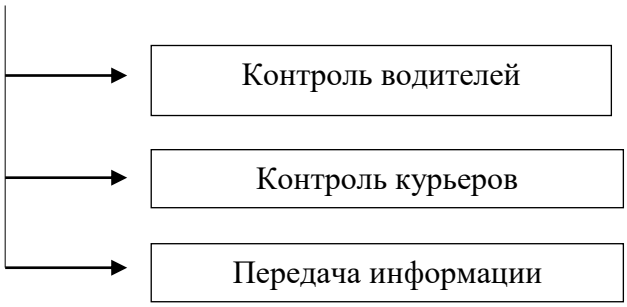


Рисунок 3.5 – Мониторинг активности сотрудников как фактор обеспечения информационной безопасности фирмы

Системе Wialon присуще передача информации:

- интеграция с 1С и другими ERP-системами;
- отчеты по каждому водителю или группе водителей;
- возможность делиться местоположением с клиентами.

Что касается контроля водителей: осуществляется контроль реального пробега; контроль соблюдения режима работы, норм труда и отдыха; Tacho View и Tacho Manager для работы с данными тахографов; возможность удаленной выгрузки DDD-файлов. Система информационной безопасности Wialon одинаково эффективно справляется с мониторингом водителей на различных объектах. За счет данного вида системы осуществляется прозрачность предпринимательской деятельности, предоставляя клиентам информацию о местоположении груза, руководитель фирмы может проверить безопасность своих работников, стимулировать дисциплину и мотивировать команду на основании объективных данных. Применение новой системы мониторинга в аспекте информационной безопасности предприятия ООО «ИнвестПрогрессЛогистик» позволяет предоставить информацию о контроле топлива. Система контроля топлива Wialon поможет : выявить использование «левых» чеков и несертифицированного топлива; подкручивание одометра, махинации с топливными картами и необоснованный пережог топлива. За счет нового информационного мониторинга возможно получать информацию в реальном времени или в форме отчетов, сравнивать реальный расход с нормами и безошибочно

определять сливы с эффективной системой мониторинга топлива. Система имеет собственный алгоритм расчета, который состоит из составляющих, представленые на рисунке 3.6.

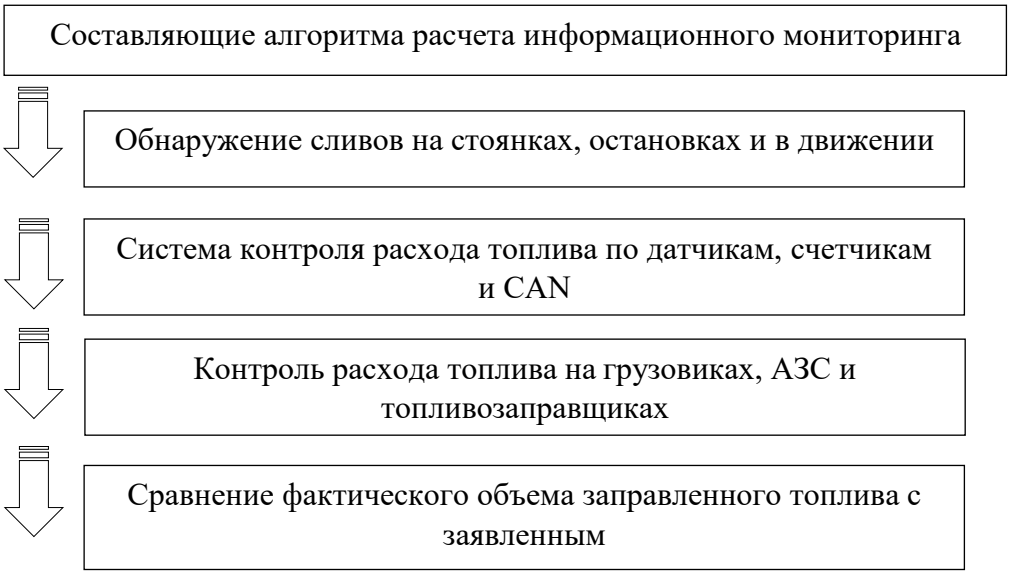


Рисунок 3.6 – Составляющие алгоритма расчета информационного мониторинга

Подчеркнем, что мониторинг топлива осуществляется в реальном времени :

- уведомления о заправках и сливах по SMS, e-mail или во всплывающих окнах;
- контроль уровня топлива онлайн в мобильном приложении.

Отдельно следует отметить преимущества мониторинговой системы – контроль территорий эксплуатации: каждый «левый рейс» и «халтура» - это дополнительный пробег и повышенный износ техники, а, значит, и лишние расходы предприятия. С информационным мониторингом Wialon фирма может быть точно проинформирована, что ценная техника и оборудование не используются на сторонних производственных объектах без ее ведома. Главный результат – экономия на техобслуживании, топливе и ликвидация хищений со стороны работников.

Система позволяет осуществлять:

- видеомониторинг и отчеты по видео;
- контроль пробега в геозонах и между геозонами;

- контроль длительности нахождения, стоянок и разгрузок в заданной геозоне ;
- фильтрация интервалов по геозонам в отчетах;
- инструмент для расчета площади и расстояния.

Система информационной безопасности также позволяет:

- осуществлять контроль разгрузки/загрузки материалов и оборудования вне геозон;
- контролировать веса после остановок и стоянок;
- контролировать открытия и закрытия дверей.

Что касается контроля доступа, то здесь осуществляется подача информации по следующим критериям:

- идентификация водителей и прицепного оборудования;
- контроль зажигания;
- учет количества посещений производственного участка;
- уведомления о несанкционированном доступе.

Таким образом, применяемый информационный продукт Wialon позволит исследуемому предприятию« ИнвестПрогрессЛогистик» решить ряд вопросов по предоставлению достоверной информации в осуществлении предпринимательской деятельности, повысив уровень информационной безопасности и соответственно, общего уровня экономической безопасности фирмы. По данным интегратора, программный продукт позволяет снизить уровень эксплуатационных расходов на 25%; на 99,9% обнаруживает« сливы »; снижает пробег на 40%; повышает оборачиваемость парка на 14-15%, предоставлять более точную отчетность на 60%. В следующем параграфе представим экономическое обоснование проекта по обеспечению информационной безопасности компании.

3.2. Экономическое обоснование проекта информационной безопасности

Установление информационной платформы Wialon будет осуществляться белгородской компанией «M2M Солюшнс»(работает с 2008 года и входит в

число российских лидеров по продажам GPS/ГЛОНАСС навигации и тахографии). Специалисты данной организации обладают уникальным опытом не только в техническом обслуживании, но и в подборе оптимальных решений под конкретные задачи заказчика.

«M2M» - комплексное решение для предприятий транспорта. Информационная платформа позволяет наладить логистические процессы, решив вопросы:

- со сливами топлива;
- контролировать производительность труда своих сотрудников;
- получать достоверную информацию.

Для предприятия планируется установить данную информационную платформу на все виды транспорта в количестве 21 шт. Стоимость одной программы-платформы составляет 5188 руб. Представим примерный прайс« M2M» Wialon для контроля автопарка в таблице 3.1.

Таблица 3.1 – Прайс «M2M» Wialon для контроля автопарка

Наименование показателя	**Кол-во**	**Ед.**	**Цена за 1 пл., руб.**
Информационная платформа Wialon	21	шт	5188
Итого за 21 шт.			108948

Представим инвестиционные затраты на монтаж и наладку оборудования в следующей таблице 3.2.

Таблица 3.2 – Прогноз инвестиционных затрат на монтаж и настройку внедряемой программы Wialon

№	**Наименование статей инвестиционных затрат**	**Сумма, руб.**
1	Монтаж блока мониторинга на ТС. Выезд к заказчику в пределах Белгорода	800
2	Демонтаж терминала мониторинга	500
3	Тарировка топливного бака, занесение в систему параметров ТС.(до 1000 литр.)	2000
4	Демонтаж ДУТ	1000
5	Переподключение оборудования, настройка	800
6	Демонтаж топливного бака	1700
Итого:		6800
Итого за автопарк:		142 800

Далее рассмотрим статьи затрат на подключение дополнительных датчиков, к ним относят:

- монтаж, подключение тревожной кнопки;
- подключение терминала мониторинга;
- монтаж Can-log, подключение, настройка;
- монтаж, подключение температурного датчика;
- монтаж микрофона в салоне ТС;
- монтаж фотоконтроля в салоне ТС;
- монтаж датчика посадки;
- монтаж реле блокировки двигателя и т.д.

Представим данные виды затрат в таблице 3.3.

Таблица 3.3 – Прогноз инвестиционных затрат на подключение дополнительных датчиков

№	Наименование статей инвестиционных затрат	Сумма, руб.
1	Монтаж, подключение тревожной кнопки	500
2	Подключение терминала мониторинга к can-шине, настройка (на прямую)	700
3	Монтаж Can-log, подключение, настройка	1000
4	Монтаж, подключение температурного датчика	1000
5	Монтаж микрофона в салоне ТС	500
6	Монтаж фотоконтроля в салоне ТС	1000
7	Монтаж датчика посадки	1000
8	Монтаж реле блокировки двигателя	800
9	Монтаж датчика работы механизмов(реле)	700
10	Монтаж датчика угла наклона, калибровка	2500
11	Монтаж датчика вращения, настройка	1800
12	Монтаж датчика моточасов	1500
13	Монтаж датчика впрыска форсунок, настройка	1300
Итого:		14300

Итого за автопарк	300300

На основании рассмотренных статей инвестиционных затрат, сведем все указанные первоначальные расходы в единую таблицу 3.4.

Таблица 3.4 – Прогнозирование общего количества единовременных затрат

№	Наименование статей инвестиционных затрат	Сумма, руб.	В % к общей сумме
1	Приобретение платформы	108948	19,7
2	Затраты на монтаж и настройку	142800	25,9
3	Подключение дополнительных датчиков	300300	54,4
Итого за автопарк		552048	100

На основании представленного прогнозирования общего количества инвестиционных затрат наблюдается следующее: наибольший удельный вес расходов приходится на подключение дополнительных датчиков 54,4%. Удельный вес затрат на монтаж и настройку платформы-мониторинга составляют 25,9%. Остальная часть в размере 19,7% приходится на приобретение информационной платформы Wialon. Соотношение инвестиционных затрат фирмы представлено на рисунке 3.7.

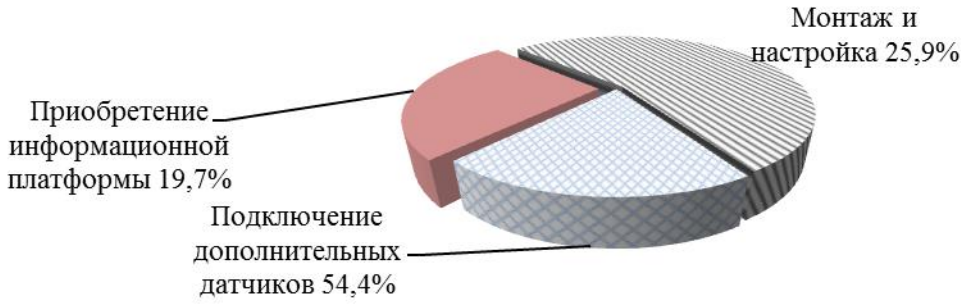


Рисунок 3.7 – Соотношение инвестиционных затрат компании «ИнвестПрогрессЛогистик»

Следует отметить, что за сопровождение информационного продукта, исследуемая фирма должна оплачивать только 20 % от общей стоимости приобретенной информационной платформы (в первый год реализации проекта внедрения информационной платформы-мониторинга для осуществления контроля потока информации и контроля активности

сотрудников« ИнвестПрогрессЛогистик» стоимость уже включена за 21 технику). Представим статьи постоянных затрат в таблице 3.5.

Таблица 3.5 – Постоянные затраты на обслуживание и техническую поддержку приборов

Наименование затрат	**Сумма в 1 год реализации проекта, руб.**	**Сумма во 2 год реализации проекта, руб.**	**Сумма в 3 год реализации проекта, руб.**
Обслуживание и техническая поддержка	0	21 790	21 790
Всего	0	21 790	21 790

На основании представленных данных мы видим, что только статья затрат «обслуживание и техническая поддержка» составляют постоянные расходы. Переменные затраты в данном проекте не предусмотрены. Подчеркнем, что программный продукт обладает простотой внедрения. Интерфейс понятный, эффективно работает в сетях любой сложности. Сопровождение проводится на всех этапах: поддержка, обучение, консалтинг и сертификация персонала.

Экономическую эффективность проекта информационной безопасности ООО «ИнвестПрогрессЛогистик» можно оценить с помощью экономии денежных средств. Рассматривая затраты предприятия за 2018 год, проведем расчет экономии денежных средств в таблице 3.6.

Таблица 3.6 – Прогнозируемый расчет экономии денежных средств, руб.

Показатель	**1 г.**	**2 г.**	**3 г.**
Затраты до внедрения информационного продукта, руб.	822 000	1088 000	1550 000
Затраты после внедрения информационного продукта, руб.	475 000	580 000	585 000
Экономия. руб.	347 000	508 000	965 000

Отметим, что затраты до внедрения программного продукта предприятия представлены на основании оперативных данных предприятия. Более иллюстративно экономия затрат представлена на рисунке 3.8.

Экономия затрат, тыс. руб.

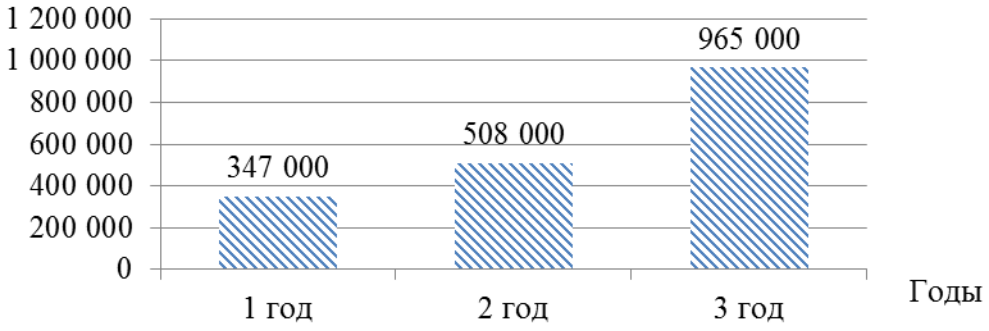


Рисунок 3.8 – Экономия затрат ООО «ИнвестПрогрессЛогистик»

Мы наблюдаем прогнозируемую экономию затрат за счет внедрения информационной платформы-мониторинга Wialon. Конечно, внедрение данного программного решения для предприятия совершенно недорогостоящее для такого предприятия, прогнозируется существенная экономия денежных средств и на основании представленного можно провести расчет денежных потоков в таблице 3.7.

Таблица 3.7 – Прогнозируемый расчет денежных потоков

Наименование показателя	**0 г.**	**1 г.**	**2 г.**	**3 г.**
Экономия, руб.	0	347 000	508 000	965 000
Инвестиционные затраты, руб.	- 552 048	0	0	0
Постоянные затраты, руб.	0	0	21790	21790
Себестоимость, руб.	0	0	21790	21790
Экономический эффект, тыс. руб.	0	347 000	486210	943 210
Чистый денежный поток, руб.	- 552 048	347 000	486 210	943 210
Чистый денежный поток нарастающим итогом, руб.	- 552 048	- 205 048	691 258	1 634 468

На основании представленных данных наблюдается положительная тенденция роста чистого денежного потока. Продемонстрируем иллюстративно тенденцию изменения чистого денежного потока фирмы на рисунке 3.9.

Чистый денежный поток. руб.

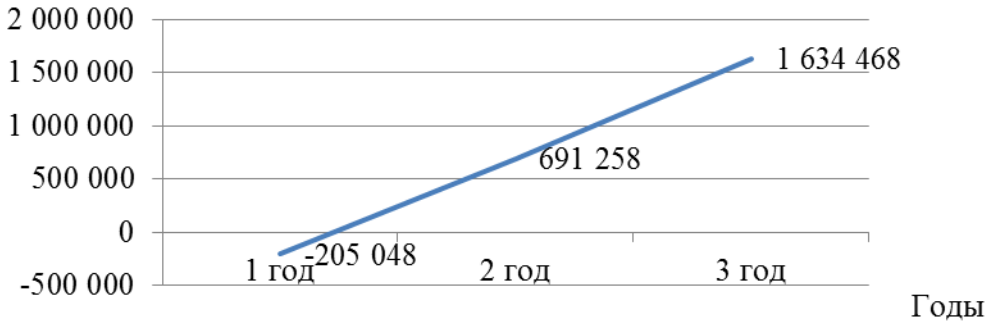


Рисунок 3.9 – Чистый денежный поток ООО «ИнвестПрогрессЛогистик»

После того, как были получены значения чистого денежного потока и чистого денежного потока нарастающим итогом, следует рассчитать чистую современную стоимость (NPV), индекс рентабельности (PI), срок окупаемости (PP), дисконтированный срок окупаемости проекта (DPP).

Отметим, что чистая современная стоимость – это чистая текущая стоимость – сумма текущих стоимостей всех прогнозированных, с учетом ставки дисконтирования, денежных потоков. При условии, если данный показатель NPV > 0, то единовременные расходы увеличат капитал предприятия и инвестиционные вложения следует осуществлять. При условии NPV<0 – доходы от предложенных инвестиций недостаточно высоки, чтобы компенсировать риск, присущий данному проекту (или с точки зрения цены капитала не хватит денег на выплату дивидендов и процентов по кредитам) и инвестиционное предложение должно быть отклонено. Рассчитаем показатель чистой современной стоимости проекта на основании следующих данных: чистых денежных потоков; денежного потока нарастающим итогом; ставки дисконтирования. Представим расчет чистой современной стоимости (NPV) проекта в таблице 3.8.

Таблица 3.8 – Расчет интегрального показателя NPV проекта, руб.

Показатель	**0**	**1**	**2**	**3**
Чистый денежный поток	- 552 048	347 000	486 210	943 210
Чистый денежный поток нарастающим итогом (аккумулированный денежный поток)	- 552 048	- 205 048	691 258	1 634 468
Ставка дисконтирования, %	-	12	12	12

Коэффициент дисконтирования	1	0,89	0,80	0,71
Дисконтированный денежный поток	- 552 048	308 830	388 968	669 679,1
Дисконтированный денежный поток нарастающим итогом(Аккумулированный дисконтированный денежный поток)	- 552 048	- 243 218	145 750	845 429,1

Отметим, что чистый денежный поток(net cash flow) – разница между положительным и отрицательным денежными потоками по конкретному виду деятельности или по хозяйственной деятельности предприятия в целом, в рассматриваемом периоде времени; дисконтиро-вание денежных потоков – это приведение стоимости потоков платежей, выполненных в разные моменты времени, к стоимости на текущий момент времени. Чистая современная стоимость (NPV) составит: - 522 048 + 308830 + 388 968 + 669 679,1 = 845 429,1 руб. Представим возможные угрозы до и после предлагаемого проекта в таблице 3.9.

Таблица 3.9 – Угрозы до и после предлагаемого проекта

Угроза до внедрения проекта	**Угроза после внедрения проекта**
Конфиденциальная информация	
1. Недостоверная информация по времени простоев	1. Контроль за временем простоев
2. Недостоверная информация по планированию и контролю соблюдения маршрута	2. Контроль по планированию и контролю соблюдения маршрута
3. Недостоверная информация по отчетам анализа продуктивности движения	3. Контроль по отчетам анализа продуктивности движения
4. Недостоверная информация по контролю качества оказываемых услуг	4. Контроль качества оказываемых услуг
5. Недостоверная информация по отчетам поездки и хронологии движения	5. Контроль по отчетам поездки и хронологии движения

На основании представленной информации мы видим совершенствование и устранение угроз. Представим основные результаты сводной оценки интегрального уровня экономической безопасности фирмы в таблице 3.10.

Таблица 3.10 – Результаты сводной оценки интегрального уровня экономической безопасности фирмы после внедрения проекта

Составляющие экономической безопасности предприятия	**Оценка (Оц) в зависимости от степени соответствия нормативу**		
	Обозначение	**2018**	**После**

			внедрения проекта
Финансовая	Уфс	0,3	0,4
Производственно-сбытовая	Упсс	0,63	0,63
Кадровая	Укс	0,33	0,5
Технико-технологическая	Уттс	0,8	0,7
Информационная	Уиб	0,36	0,6
Сводный интегральный уровень экономической безопасности фирмы	ИУэб	0,47	0,63

По предварительным подсчетам, сводный интегральный уровень экономической безопасности фирмы« ИнвестПрогрессЛогистик» вырастет на 16%.Внедрение платформы-мониторинга в деятельность предприятия« ИнвестПрогрессЛогистик» - ключевой элемент при построении в организации эффективной системы управления информационной безопасностью. В рамках произведенных расчетов наблюдаем прогнозируемую экономию затрат за счет внедрения программного продукта Wialon. Конечно, внедрение данного программного решения совершенно недорогостоящее для такого предприятия, прогнозируется существенная экономия денежных средств. Внедрение нового программного продукта характеризуется большим количеством положительных возможностей для рассматриваемой организации. Также внедрение нового программного решения позволит снизить затраты ориентировочно на 25 %.

3.3. Совершенствование направления обеспечения информационной безопасности компании

В предыдущем параграфе была предложена платформа-мониторинг, которая предоставляла достоверную информацию, с которой непосредственно работают сотрудники(водители транспортных средств). Помимо, в организации существует ряд сотрудников, которые, непосредственно, работают в офисе с базами данных, с ценной информацией. Если его уровень недопустим для предприятия, оно внедряет защитные меры, чтобы снизить риск до приемлемого уровня. Однако систем или сред, которые имеют

нулевой риск, не существует – всегда есть некоторый остаточный риск. Уровень остаточного риска должен быть приемлемым для предприятия.

По данным второй главы, информационная система «ИнвестПрогрессЛогистик» не защищена и необходимо принять меры по снижению остаточного риска до приемлемого уровня и по усилению защиты распределенной информационной системы. Матрица рисков представлена в таблице 3.11.

Таблица 3.11 – Матрица рисков (согласно рекомендациям NIST «Risk Management Guide for Information Technology Systems»)

Вероятность атаки (Р)	**Ущерб**		
	Низкий **0 < У < = 10 (%)**	**Средний** **10 < У < = 50 (%)**	**Высокий** **50 < У < = 100 (%)**
Высокая (0,5 < Р < = 1)	Низкий 5 < R < = 10 (%)	Средний 10 < R < = 50 (%)	Высокий 50 < У < = 100 (%)
Средняя (0,1 < Р < = 0,5)	Низкий 1 < R < = 5 (%)	Средний 5 < R < = 25(%)	Высокий 50 < R < = 100 (%)
Низкая (0 < Р < = 0,1)	Низкий 0 < R < = 1 (%)	Низкий 0 < R < = 5 (%	Низкий 0 < R < = 10 (%)

В целях контроля офисных сотрудников в аспекте информационной безопасности, предлагаем предприятию установить программу StaffCop. Внедряемая программа позволяет проводить тотальный контроль. Схема контроля сотрудников представлена на рисунке 3.10.

Рисунок 3.10 – Схема контроля сотрудников в целях повышения уровня информационной безопасности фирмы

Существует перечень статей уголовного кодекса Российской Федерации, которые предусматривают ответственность за некоторые виды деяний, часто встречающихся в частных компаниях, в рамках которых обеспечение StaffCop позволит выявить угрозы, оказывающие влияние на информационную безопасность ООО «ИнвестПрогрессЛогистик»: причинение имущественного ущерба путем обмана или злоупотребления доверием, злоупотребление полномочиями; незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. Представим примерную стоимость лицензионного продукта StaffCop в таблице 3.12.

Таблица 3.12 – Планируемая стоимость лицензионного продукта StaffCop

№ п/п	**Наименование продукта**	**Стоимость установки на 1 компьютер, руб.**	**Общее число компьютеров, шт.**	**Общая сумма, руб.**
1	Лицензионный продукт технической программы StaffCop (бессрочная лицензия)	3 800	10	38 000
2	Пакет продления доступа к обновлениям на 3 года	2 145	10	21 450
3	Премиум поддержка на 2 года	1 200	10	12 000
Итого				71 450

Кроме того, необходимо отметить основные угрозы, также планируемый результат при внедрении технической программы StaffCop для предприятия ООО «ИнвестПрогрессЛогистик». Следует подчеркнуть, что техническая

программа StaffCop обеспечивает полный контроль документооборота и позволяет вовремя предупредить утечку конфиденциальной информации. Под наблюдением системы находятся все информационные каналы.

Контроль за информацией и предотвращение утечек - основные задачи, которые стоят перед данной системой. StaffCop - комплексное программное решение для информационной защиты бизнеса от внутренних угроз, функционал которого развивается в нескольких направлениях. Кроме того, в случае выявления противоправных действий в части попытки кражи конфиденциальной информации, злоупотреблением должностными полномочиями и т.д., можно составить прогноз экономии за счет внедрения программного продукта StaffCop. Планируемый результат после внедрения технической программы StaffCop для компании «ИнвестПрогрессЛогистик» представлен в табл. 3.13.

Таблица 3.13 – Планируемый результат после внедрения технической программы StaffCop для компании «ИнвестПрогрессЛогистик»

Угроза до внедрения проекта	**Планируемый результат**
Рабочее место сотрудника (конфиденциальная информация)	
1. Физический доступ нарушителя к рабочему месту и, как следствие к необходимой информации (получение и разглашение конфиденциальной информации и информации, составляющей коммерческую, налоговую или банковскую тайну третьим лицам).	1. Постоянный контроль за рабочим местом
2. Утрата или повреждение конфиденциальной информации при помощи специализированных программ, вирусов, а также вследствие действий третьих лиц	2. Минимизация возможности утраты или повреждения конфиденциальной информации при помощи специализированных программ, вирусов, а также вследствие действий третьих лиц.
3. Причинение ущерба (имущественного, финансового, а также кадрового) ООО «ИнвестПрогрессЛогистик» путем обмана или злоупотребления доверием.	3. Минимизация ущерба(имущественного, финансового, а также кадрового) ООО «ИнвестПрогрессЛогистик» путем предотвращения возможного обмана или злоупотребления доверием
4. Причинение ущерба (имущественного, финансового, а также кадрового) ООО «ИнвестПрогрессЛогистик» путем злоупотребления должностными полномочиями.	4. Минимизация ущерба(имущественного, финансового, а также кадрового) ООО «ИнвестПрогрессЛогистик» путем злоупотребления должностными полномочиями.
5. Причинение ущерба (имущественного, финансового, а также кадрового) ООО «ИнвестПрогрессЛогистик» путем	5. Минимизация ущерба (имущественного, финансового, а также кадрового) ООО «ИнвестпрогрессЛогистик» путем

коммерческого подкупа сотрудников предприятия	коммерческого подкупа сотрудников предприятия
6. Причинение ущерба (имущественного, финансового, а также кадрового) ООО «ИнвестПрогрессЛогистик» путем халатности сотрудников.	6. Минимизация ущерба(имущественного, финансового, а также кадрового) ООО «ИнвестПрогрессЛогистик» путем халатности сотрудников

Планируемые показатели нарушений в аспекте информационной безопасности после внедрения технической программы StaffCop для предприятия ООО «ИнвестПрогрессЛогистик» указаны в таблице 3.14

Таблица 3.14 – Планируемые показатели нарушений до и после внедрения технической программы StaffCop для предприятия ООО «ИнвестПрогрессЛогистик»

Показатель	**2016 г.**	**Ошибка! ущерб, руб.**	**2017 г.**	**Ошибка! ущерб, руб.**	**2018г.**	**Ошибка! ущерб, тыс.руб.**	**2019 г.**	**Ориентировочный ущерб, тыс.руб.**
Количество выявленных правонарушений, шт.	3	120 000	2	58 000	2	592 000	0	0
Случаи возникновения конфликтов интересов, шт.	2	57 000	1	44 000	1	69	0	0
Выявленные случаи неблагонадежности контрагентов, шт.	1	143 000	1	212 000	-	161 000	-	-
Итого	6	320 000	4	328 000	2	822 000	0	0

На основании анализа выявленных правонарушений на предприятии ООО «ИнвестПрогрессЛогистик» за последние три года, ориентировочная экономия после внедрения технической программы StaffCop за три года может составить около 1 470 тыс. рублей.

Таким образом, в целях повышения уровня информационной безопасности предприятия были предложены два мероприятия: проект платформы-мониторинга Wialon – который позволяет контролировать

водителей и их транспортные средства, предоставляя достоверную информацию; совершенствование информационной безопасности за счет программного продукта StaffCop. Представленные мероприятия повышают уровень экономической безопасности фирмы, в том числе, и информационный, что является положительным моментом в осуществлении предпринимательской деятельности.

ЗАКЛЮЧЕНИЕ

Таким образом, в данной работе были решены следующие задачи:

- изучена интерпретация информационной безопасности;
- представлена классификация угроз информационной безопасности и способы защиты информации;
- рассмотрены норматвино-правовые акты в области информационной безопасности и защиты информации;
- представлена организационно-экономическая характеристика предприятия;
- проведен анализ системы экономической безопасности предприятия;
- проведена оценка системы защиты информации на предприятии;
- предложена общая характеристика проекта по обеспечению информационной безопасности предприятия;
- экономически обоснован проект информационной безопасности;
- предложено совершенствование направления обеспечения информационой безопасности компании, сделаны выводы.

Информационная безопасность характеризуется состоянием защищенности информационных потоков и поддерживающей инфраструктуры от нежелательных воздействий естественного или искусственного характер. Данные воздействия могут нанести огромный ущерб субъектам информационных отношений, особенно это касается владельцев и пользователей информации и поддерживающей инфраструктуры. Что касается защиты информации, то она может быть представлена как комплекс мер, который направлен на формирование информационной безопасности. К

доступности наиболее связанных эффективному способу органов защиты сохранность информации относится такому криптостойкий применении алгоритм шифрования при система передаче внедрит данных . Система необходимость зашифровывает утечки саму информацию, а не несколько только контролировать доступ к ней, что актуально и для изучены безопасности такая банковской информации.

Предприятие «ИнвестПрогрессЛогистик» создано на основании Гражданского Кодекса Российской Федерации. Юридический адрес фирмы: 308002, г. Белгород, проспект Б. Хмельницкого, д. 133, оф. 32-а. Предприятие прошло регистрацию в мае 2011 года Инспекцией Федеральной Налоговой Службы по г. Белгороду.

Основной вид деятельности заключается в вспомогательной и дополнительной транспортной деятельности, организации перевозок грузов. Наличие собственного современного автопарка и высокий профессионализм сотрудников позволяют фирме обеспечивать качественную, оперативную и безопасную транспортировку грузов по Белгородской области, территории Российской Федерации по конкурентоспособной цене в строго оговоренные сроки. Специалисты фирмы предложат оптимальные маршруты перевозки, исходя из условий и предъявляемых требований.

Также следует отметить, что исследуемая фирма предоставляет услуги по комплексным поставкам различных стриотельных материалов фирмам строительно-дорожной и строительной индустрии на территории Центрального Черноземья(Воронежская область, Курская область, Старый Оскол, Липецк, непосредственно вся территория Белгородчины). Фирма характеризуется достаточным опытом в сотрудничестве со многими крупными строительно-дорожными и строительными предприятиями области. Это говорит о том, что исследуемая фирма надежна и оперативна.

На основании представленных данных в последний год наблюдается незначительное повышение интегрального уровня экономической безопасности предприятия: технико-технологическая составляющая

уменьшилась в 2018 году по сравнению с предыдущим годом на 0,1; кадровая составляющая в 2018 году на 0,67. Финансовая составляющая увеличилась на 0,2 норматива, однако характеризуется неудовлетворительной ситуацией в осуществлении предпринимательской деятельности фирмы.

По предварительным подсчетам, сводный интегральный уровень экономической безопасности фирмы «ИнвестПрогрессЛогистик» вырастет на 16%.Внедрение платформы-мониторинга в деятельность предприятия «ИнвестПрогрессЛогистик» - ключевой элемент при построении в организации эффективной системы управления информационной безопасностью. В рамках произведенных расчетов наблюдаем прогнозируемую экономию затрат за счет внедрения программного продукта Wialon. Конечно, внедрение данного программного решения совершенно недорогостоящее для такого предприятия, прогнозируется существенная экономия денежных средств. Внедрение нового программного продукта характеризуется большим количеством положительных возможностей для рассматриваемой организации. Также внедрение нового программного решения позволит снизить затраты ориентировочно на 25 %.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Федеральный закон Российской Федерации от 27 июля 2016 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29.11.1994 № 77-ФЗ «Об обязательном экземпляре документов».

3. Закон РФ от 27.12.1991 № 2124 – 1 «О средствах массовой информации».

4. Закон РФ от 21.07.1993 № 5485 – 1 «О государственной тайне».

5. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне ».

6. Федеральный закон от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»;

7. Федеральный закон от 12.05.2009 № 95-ФЗ «О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами»;

8. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

9. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;

10. Федеральный закон от 28.07.2012 № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты».

11. Государственная стратегия экономической безопасности Российской Федерации(Основные положения) – Указ Президента Российской Федерации от 29 апреля 2016 г. № 608 // Консультант Плюс.

12. Концепция долгосрочного социально-экономического развития Российской Федерации до 2020 года– Распоряжение Правительства Российской Федерации от 17 ноября 2016 г. № 1662-р // Консультант Плюс.

13. О безопасности. – Федеральный Закон РФ от 28 декабря 2014 г. № 390-ФЗ // Консультант Плюс.

14. Абалкин, Л. Экономическая безопасность России: угрозы и их отражение / Л. Абалкин // Вопросы экономики. - 2016. - № 12. - С. 48-59.

15. Абдурахманов, А. А. Современные подходы к организации мониторинга криминологической ситуации в регионе / А.А. Абдурахманов //Право и политика. – 2015. - №6.

16. Барт, А. А. Механизм обеспечения экономической безопасности: основные виды экономической безопасности / А. А. Барт // Российское предпринимательство. – 2016 .– № 11, вып. 1 .– С. 4-9.

17. Биячуев, Т.А. Безопасность корпоративных сетей / Т.А. Биячуев. - СПб: СПб ГУ ИТМО, 2016.- 161 с.

18. Борисов Н.Е., – Разработка компьютеризированной подсистемы оценки рисков операций с пластиковыми картами в условиях ПИБ. [Электронный ресурс] – Режим доступа: http://www.masters.donntu.org/2016 /kita/borisov/diss/index.htm

19. Вихорев, С. Как определить источники угроз / С. Вихорев, Р.Кобцев //Открытые системы. - 2016. - №07-08.-С.43.

20. Волчков, А. Современная криптография / А.Волчков // Открытые системы. - 2015. - № 07-08. - С.48.

21. Габети, А. В. Теоретические основы обеспечения экономической безопасности малых и средних предприятий / А. В. Габети // Известия Санкт-Петербургского университета экономики и финансов. – 2016 .– № 5 (65) .– С. 100-103

22. Галатенко, В.А. Основы информационной безопасности. - М.: Интуит, 2015. – 340 с.

23. Гмурман, А.И. Информационная безопасность/ А.И. Гмурман - М.: «БИТ-М», 2015. – 387 с.

24. Конахович, Г. Защита информации в телекоммуникационных системах предприятия / Г. Конахович. - М.: МК-Пресс, 2015. – 356 с.

25. Коржов, В. Стратегия и тактика защиты / В.Коржов //Computerworld Россия. - 2016. - №14. - С.26.

26. Каранина, Е.В. Формирование и обеспечение финансово-экономической безопасности на основе критериев риск-системы: комплексный подход: монография / Е.В. Каранина. - Киров: Типография« Старая Вятка», 2015. – 400 с.

27. Каранина, Е.В.Экспресс-диагностика уровня экономической безопасности / Е. В. Каранина // Экономика и управление: проблемы и решения. –№ 12. – 2015 г. – С.146-153.

28. Кашин А.В. Экономическая безопасность предприятия: управленческие решения: диссертация. - М.: Бератор-Паблишин, 2016. – 167 с.

29. Козаченко А.В., Пономарев В.П., Ляшенко А.Н. Экономическая безопасность предприятия: сущность и механизм обеспечения. Монография. – К.: Либра, 2017. – 280 с.

30. Комплексная безопасность бизнеса в условиях экономической нестабильности [Электронный ресурс] : материалы научно-практической конференции / М-во образования и науки Рос. Федерации, С.-Петерб. гос. экон. ун-т, Каф. вычислит. систем и программирования ; [отв. ред. Е.В.Стельмашонок, С.Н.Максимов] .– Санкт-Петербург : Изд-во СПбГЭУ, 2016 .– 151 с.

31. Кузнецова Е.И. Экономическая безопасность предприятия и конкурентоспособность. – М.: ЮНИТИ, 2017. – 239 с.

32. Кузнецов И.Н. Бизнес-безопасность. – М.: ИТК «Дашков и К°», 2016. – 416 с.

33. Литвиненко А.Н., Ковтунова С.Ю. Разработка типовой структуры механизма обеспечения экономической безопасности // Вестник Санкт-Петербургского университета МВД России. – 2016. – № 4. – С. 137-144.

34. Логинов М.П. Экономические механизмы: сущность, классификация, кибернетический подход // Проблемы теории и практики управления. – 2015. - № 9. - С. 94-102.

35. Мак-Мак В.П. Безопасность предприятия. – М.: Изд-во «КНГ», 2017. – 440 с.

36. Матвеев Н.В. Экономическая безопасность России: системно-правовое исследование. - М.: МПСИ, МОДЭК, 2016. - 56 с.

37. Лебедева Н.А. Экономическая безопасность предприятия. – М.: Изд-во «МАБИВ», 2018. – 162 с.

38. Новак Б.Н. Бизнес в России. Руководство по технике безопасности. – СПб.: Питер, 2016. – 240 с.

39. Одинцов А.А. Экономическая и информационная безопасность предпринимательства. – М.: Изд-во «Академия», 2016. – 336 с.

40. Прокопов Б.И. Экономическая глобализация и проблемы национальной и международной безопасности// Проблемы современной экономики. – 2015. – № 3. – С. 50-60

41. Сенчагов В.К. Экономическая безопасность России: общий курс. - М.: Бином. Лаборатория знаний, 2018. - 815 с.

42. Любецкий, Р. В. Совершенствование институциональной системы формирования человеческого капитала в современной России / Р.В. Любецкий: дис. ... канд. экон. наук. М., 2016. – 520 с.

43. Любимова, М.В. Проблемы оценки социально-экономического потенциала / М. В. Любимов // Региональная экономика: теория и практика.– № 4. – 2015 г. – С. 13-24.

44. Лыкин, С. Развитие экономики России и ее структуризация как гарантия экономической безопасности // Вопросы экономики. – № 12. – 2016– С. 45-51.

45. Мельников, В. Защита информации в компьютерных системах / В.Мельников - М.: Финансы и статистика, Электронинформ, 2016. – 400 с.

46. Мельников В.П., – Информационная безопасность и защита информации / В.П. мельников, С.А. Клейменов, А.М. Петраков. – 3–е изд., стер. – М.: Издательский центр «Академия», 2016. – 336 с.

47. Нив Генри Организация как система: Принципы построения устойчивого бизнеса Эдвардса Деминга [Электронный ресурс] / Генри Нив ; [пер. с англ., науч. ред.: Ю. Рубаник, Ю. Адлер, В. Шпер] . – Москва : Альпина Паблишер, 2015. – 370 с.

48. 31. Низовкина Н.Г. Управление затратами предприятия (организации) [Электронный ресурс]: Учебное пособие / Низовкина Н.Г. – 2-е изд., испр. и доп .– М. : Издательство Юрайт, 2017 .– 185 с.

49. Никуленко Е.Д. Разработка модели для оценки потерь, связанных с реализацией угроз и уязвимостей для информационных систем. [Электронный ресурс] – Режим доступа: http://masters.donntu.org/2011/fknt/nikulenko/ diss/index.htm

50. Острейковский, В.А. Информатика: Учеб. пособие для студ. сред. проф. учеб. Заведений/ В.А. Острейковский. - М.: Высш. шк., 2016. – 319 с.

51. Рахимов, О. Р. Содержание понятия экономическая безопасность // Научный вестник МГИИТ. М., Вып. 5(13). 2016. – С.42-50.

52. Сенчагов, В.К. Экономическая безопасность России: Общий курс / В.К. Сенчагов. – М.: Бином. Лаборатория знаний, 2018. – 815 с.

53. Скачко, Г.А., Никандрова Л.К. Роль анализа и диагностики финансово-хозяйственной деятельности в оценке экономической безопасности организации (Текст) / Г.А. Скачко // Аудиторские ведомости. - 2016. – №7. – С. 54-63.

54. Суглобов, А.Е. Экономическая безопасность предприятия: Учебное пособие / А.Е. Суглобов, С.А. Хмелев, Е.А. Орлова. - М.: ЮНИТИ, 2015. – 271 с.

55. Тамбовцев В.Л. Экономическая безопасность хозяйственных систем: структура проблемы// Вестник МГУ. – 2015. - №5. – С. 88-94

56. Трошин Д.В. Безопасность предприятия: смысл, онтология, оценка: монография. – Тверь: Твер. гос. ун-т, 2015. – 212 с.

57. Уразгалиев, В.Ш. Экономическая безопасность. Учебник и практикум. – М.: Юрайт, 2016. – 376 с.

58. Управление бизнесом: сборник статей. – Нижний Новгород: Изд-во Нижегородского университета, 2015. – 243 с.

59. Фирсова О.А. Экономическая безопасность предприятия. – М.: ЮНИТИ-ДАНА, 2015. – 385 с.

60. Хлутков А.Д. Роль службы безопасности предприятия в обеспечении экономической безопасности бизнеса // Известия Санкт-Петербургского государственного экономического университета. - № 2. - С. 34-40.

61. Шаваев А.Г. Экономическая безопасность: энциклопедия. – М.: Правовое просвещение, 2018. – 288 с.

62. Шинкаренко, П. Технологическая и экономическая безопасность России : проблемы и решения // Проблемы теории и практики управления. 2016. №12. С. 116-122.

63. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. – СПб.: Алетейя, 2016. – 306 с.

64. Черенков, В.Е. Современные направления и механизмы обеспечения экономической безопасности / В.Е. Черенков. – Брянск: БФ ОРАГС, 2016. – 174 с.

65. Черняк В.З. Управление предпринимательскими рисками в системе экономической безопасности. Теоретический аспект: монография. – М.: ЮНИТИ-ДАНА, 2015. – 159 с.

66. Экономическая безопасность хозяйственных систем : учебник / под общ. ред. проф. А. В. Колосова. - М.: Изд-во РАГС, 2018. - 446 с.

67. Эриашвили, Н.Д. Экономическая безопасность: Учебное пособие для студентов вузов, обучающихся по специальностям экономики и управления. - М.: ЮНИТИ-ДАНА, 2016. - 295 с.

68. Ялмаев Р. А., Эскиев М. А., Бексултанова А. И. Инвестиционная безопасность предприятия и направления его укрепления // Молодой ученый. – 2015. – №21. — С. 523-525. — URL https://moluch.ru/archive/101/22811/ (дата обращения: 11.01.2018).

69. Янкина, И.А. Финансовая безопасность предприятий: необходимость системного подхода и участия банков (Текст)/ И.А. Янкина // Банковское право. – 2016. – №1. – 268 с.

70. Яскевич, В.И. Организационные основы безопасности фирмы / В.И. Яскевич. – М.: ось-89, 2017. – 368 с.

ПРИЛОЖЕНИЯ

Приложение А

Утверждён:
протоколом № 2 общего
собрания
учредителей
ООО «ИнвестПрогрессЛогистик»
от 17мая 2011 г.

УСТАВ
ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ИНВЕСТПРОГРЕССЛОГИСТИК»

Белгород 2011

Продолжение приложения А

Глава I. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные положения.

1.1. Общество действует на основании Гражданского кодекса Российской Федерации, Федерального закона «Об обществах с ограниченной ответственностью» (далее – Федеральный закон), и настоящего Устава (далее – устав).

1.2. Участники общества не отвечают по его обязательствам и несут риск убытков, связанных с деятельностью общества, в пределах стоимости принадлежащих им долей в уставном капитале общества.

Участники общества, оплатившие доли не полностью, несут солидарную ответственность по обязательствам Общества в пределах стоимости неоплаченной части принадлежащих им долей в уставном капитале Общества.

1.3. Общество имеет в собственности обособленное имущество, учитываемое на его самостоятельном балансе, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, исполнять обязанности, быть истцом и ответчиком в суде.

Общество может иметь гражданские права и исполнять гражданские обязанности, необходимые для осуществления любых видов деятельности, не запрещенных федеральными законами, если это не противоречит предмету и целям деятельности.

1.4. Общество имеет полное и сокращенное фирменное наименование на русском языке. Общество вправе иметь также полное и (или) сокращенное фирменное наименование на языках народов Российской Федерации и (или) иностранных языках.

Полное фирменное наименование общества: Общество с ограниченной ответственностью «ИнвестПрогрессЛогистик».

Сокращенное фирменное наименование общества: ООО «ИнвестПрогрессЛогистик».

1.5. **Место нахождение Общества: 308002, г. Белгород, пр-т Б. Хмельницкого, д. 131, оф. 2-36.**

1.6. Уставный капитал общества составляется из номинальной стоимости долей его участников и составляет **50 000 (пятьдесят тысяч) рублей.**

1.7. Действительная стоимость доли участника общества соответствует части стоимости чистых активов общества, пропорциональной размеру его доли.

1.8. Общество может создавать филиалы и открывать представительства.

Статья 2. Цели и виды деятельности общества.

2.1. Основная цель деятельности общества – извлечение прибыли.

2.2. Основными видами деятельности общества являются:

- вспомогательная и дополнительная транспортная деятельность; организация перевозок грузов;
- другие, не запрещённые законом виды деятельности.

2.3. При выполнении работ, связанных с секретными материалами, Общество обязано по своему статусу исполнять требования Закона РФ «О государственной тайне» от 21 сентября 1993 года и другие нормативные акты по вопросам защиты государственной тайны.

2.4. Отдельными видами деятельности, перечень которых определяется федеральным законом, общество может заниматься только на основании специального разрешения (лицензии). Если условиями предоставления специального разрешения (лицензии) на осуществление определенного вида деятельности предусмотрено требование осуществлять такую деятельность как исключительную, общество в течение срока действия специального разрешения (лицензии) вправе осуществлять только виды деятельности, предусмотренные специальным разрешением (лицензией), и сопутствующие виды деятельности.

Статья 3. Ответственность общества

3.1. Общество несет ответственность по своим обязательствам всем принадлежащим ему имуществом.

3.2. Общество не отвечает по обязательствам своих участников.

3.3. В случае несостоятельности (банкротства) общества по вине его участников или по вине других лиц, которые имеют право давать обязательные для общества указания либо иным образом имеют возможность определять его действия, на указанных участников или других лиц в случае недостаточности имущества общества может быть возложена субсидиарная ответственность по его обязательствам.

3.4. Российская Федерация, субъекты Российской Федерации и муниципальные образования не несут ответственности по обязательствам общества, равно как и общество не несет ответственности по обязательствам Российской Федерации, субъектов Российской Федерации и муниципальных образований.

3.5. Общество обеспечивает своим работникам безопасные условия труда и несет ответственность за ущерб, причиненный их жизни и здоровью в соответствии с законодательством РФ.

Статья 4. Счета Общества, печать бланки, штампы общества и товарные знаки

4.1. Общество считается созданным как юридическое лицо с момента его государственной регистрации в порядке, установленном законодательством. Общество создается без ограничения срока деятельности.

4.2. Общество вправе в установленном порядке открывать банковские счета на территории Российской Федерации и за ее пределами.

4.3. Общество должно иметь круглую печать, содержащую его полное фирменное наименование на русском языке и указание на место нахождения общества. Печать общества может содержать также фирменное наименование общества на любом языке народов Российской Федерации и (или) иностранном языке.

Общество вправе иметь штампы и бланки со своим фирменным наименованием, собственную эмблему, а также зарегистрированный в установленном порядке товарный знак и другие средства индивидуализации.

Продолжение приложения А

Статья 5. Филиалы и представительства общества

5.1. Общество может создавать филиалы и открывать представительства по решению общего собрания участников общества, принятому большинством не менее двух третей голосов от общего числа голосов участников общества.

Создание обществом филиалов и открытие представительств на территории Российской Федерации осуществляются с соблюдением требований Федерального закона и иных федеральных законов, а за пределами территории Российской Федерации также в соответствии с законодательством иностранного государства, на территории которого создаются филиалы или открываются представительства, если иное не предусмотрено международными договорами Российской Федерации.

5.2. Филиалом общества является его обособленное подразделение, расположенное вне места нахождения общества и осуществляющее все его функции или их часть, в том числе функции представительства.

5.3. Представительством общества является его обособленное подразделение, расположенное вне места нахождения общества, представляющее интересы общества и осуществляющее их защиту.

5.4. Филиал и представительство общества не являются юридическими лицами и действуют на основании утвержденных обществом положений. Филиал и представительство наделяются обществом имуществом.

Руководители филиалов и представительств общества назначаются обществом и действуют на основании его доверенности.

Филиалы и представительства общества осуществляют свою деятельность от имени общества. Ответственность за деятельность филиала и представительства общества несет общество.

Статья 6. Дочерние и зависимые общества

6.1. Общество может иметь дочерние и зависимые хозяйственные общества с правами юридического лица, созданные на территории Российской Федерации в соответствии с Федеральным законом и иными федеральными законами, а за пределами территории Российской Федерации также в соответствии с законодательством иностранного государства, на территории которого создано дочернее или зависимое хозяйственное общество.

Статья 7. Участники общества, их права и обязанности

7.1. Участниками общества могут быть граждане и юридические лица. Федеральным законом может быть запрещено или ограничено участие отдельных категорий граждан в обществах..

7.2. Участники Общества вправе:

7.2.1. Участвовать в управлении делами Общества в порядке, установленном настоящим Уставом и действующим законодательством Российской Федерации.

7.2.2. Получать информацию о деятельности Общества и знакомиться с его бухгалтерскими книгами и иной документацией.

7.2.3. Принимать участие в распределении прибыли.

7.2.4. Продать или осуществить отчуждение иным образом своей доли или части доли в уставном капитале общества одному или нескольким участникам данного общества либо другому лицу в порядке, предусмотренном настоящим Уставом и Федеральным законом.

7.2.5. Выйти из общества путем отчуждения своей доли обществу, если такая возможность предусмотрена уставом общества, или потребовать приобретения обществом доли в случаях, предусмотренных настоящим Уставом и Федеральным законом.

7.2.6. Получить в случае ликвидации Общества часть имущества, оставшегося после расчетов с кредиторами, или его стоимость.

7.2.7. Участники Общества имеют также другие права, предусмотренные настоящим Уставом и действующим законодательством Российской Федерации.

7.3. Помимо прав, предусмотренных настоящим Уставом и действующим законодательством Российской Федерации по решению Общего Собрания Участников Общества, принятому всеми Участниками Общества единогласно, всем Участникам Общества или конкретному Участнику могут быть предоставлены иные права (дополнительные права) Участника (Участников) Общества.

Дополнительные права, предоставленные определенному Участнику Общества, в случае отчуждения его доли или части доли к приобретателю доли или части доли не переходят.

Прекращение или ограничение дополнительных прав, предоставленных всем Участникам Общества, осуществляется по решению Общего Собрания Участников Общества, принятому всеми Участниками Общества единогласно. Прекращение или ограничение дополнительных прав, предоставленных определенному Участнику Общества, осуществляется по решению Общего Собрания Участников Общества, принятому большинством не менее двух третей голосов от общего числа голосов Участников Общества, при условии, если Участник Общества, которому принадлежат такие дополнительные права, голосовал за принятие такого решения или дал письменное согласие.

Участник Общества, которому предоставлены дополнительные права, может отказаться от осуществления принадлежащих ему дополнительных прав, направив письменное уведомление об этом Обществу. С момента получения Обществом указанного уведомления дополнительные права Участника Общества прекращаются.

7.4. Участники Общества обязаны:

7.4.1. Оплачивать доли в уставном капитале общества в порядке, в размерах и в сроки, которые предусмотрены Федеральным законом «Об обществах с ограниченной ответственностью», действующим законодательством и договором об учреждении Общества.

7.4.2. Не разглашать конфиденциальную информацию о деятельности Общества.

7.4.3. Участники Общества несут и другие обязанности, предусмотренные настоящим Уставом и действующим законодательством Российской Федерации.

7.5. Помимо обязанностей, предусмотренных настоящим Уставом и действующим законодательством Российской Федерации по решению Общего Собрания Участников Общества, принятому всеми Участниками Общества

единогласно, на всех Участников Общества могут быть возложены иные обязанности (дополнительные обязанности) Участника (Участников) Общества. Возложение дополнительных обязанностей на определенного Участника Общества осуществляется по решению Общего Собрания Участников Общества, принятому большинством не менее двух третей голосов от общего числа голосов Участников Общества, при условии, если Участник Общества, на которого возлагаются такие дополнительные обязанности, голосовал за принятие такого решения или дал письменное согласие.
Дополнительные обязанности, возложенные на определенного Участника Общества, в случае отчуждения его доли или части доли к приобретателю доли или части доли не переходят.
Дополнительные обязанности могут быть прекращены по решению Общего Собрания Участников Общества, принятому всеми Участниками Общества единогласно.
7.6. Участники Общества, доли которых в совокупности составляют не менее чем десять процентов Уставного Капитала Общества, вправе требовать в судебном порядке исключения из Общества Участника, который грубо нарушает свои обязанности либо своими действиями (бездействием) делает невозможной деятельность Общества или существенно ее затрудняет.
7.7. Все изменения персонального состава Участников Общества влекут за собой соответствующие изменения в списках участников Общества.
7.8. Число Участников Общества не должно быть более пятидесяти. В случае если число Участников Общества превысит установленный настоящим пунктом предел, Общество в течение года должно преобразоваться в открытое акционерное общество или в производственный кооператив. Если в течение указанного срока Общество не будет преобразовано и число Участников Общества не уменьшится до установленного настоящим пунктом предела, оно подлежит ликвидации в судебном порядке по требованию органа, осуществляющего государственную регистрацию юридических лиц, либо иных государственных органов или органов местного самоуправления, которым право на предъявление такого требования предоставлено федеральным законом.

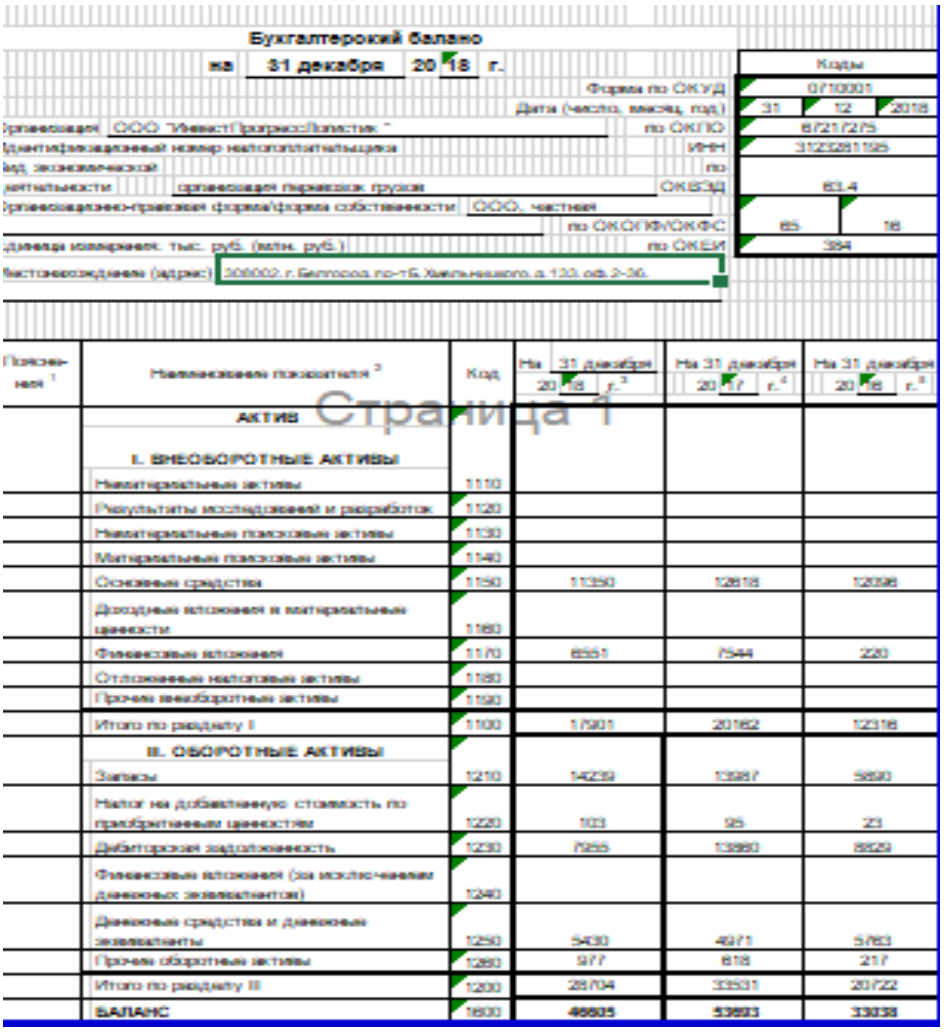
Приложение Б

Отчет о прибылях и убытках

за январь-декабрь 2018 г.			Коды
		Форма по ОКУД	0710002
		Дата (число, месяц, год)	31 12 2018
Организация ООО "ИнвестПрогрессЛогистик"		по ОКПО	67217275
Идентификационный номер налогоплательщика		ИНН	3123281195
Вид экономической деятельности	организация перевозок грузов	по ОКВЭД	63.4
Организационно-правовая форма/форма собственности	ООО, частная	по ОКОПФ/ОКФС	65 16
Единица измерения: тыс. руб. (млн. руб.)		по ОКЕИ	384

Пояснения [1]	Наименование показателя [2]	Код	2018 г. [3]	2017 г. [4]
	Выручка [5]	2110	46822	38456
	Себестоимость продаж	2120	35398	37651
	Валовая прибыль (убыток)	2100	11424	805
	Коммерческие расходы	2210		
	Управленческие расходы	2220		
	Прибыль (убыток) от продаж	2200	11424	805
	Доходы от участия в других организациях	2310		
	Проценты к получению	2320		
	Проценты к уплате	2330		
	Прочие доходы	2340		
	Прочие расходы	2350	621	505
	Прибыль (убыток) до налогообложения	2300	10803	300
	Текущий налог на прибыль	2410	2160	161
	в т.ч. постоянные налоговые обязательства (активы)	2421		
	Изменение отложенных налоговых			

Приложение В



Бухгалтерский баланс

на 31 декабря 2018 г.

		Коды
	Форма по ОКУД	0710001
	Дата (число, месяц, год)	31 | 12 | 2018
Организация: ООО "ИнвестПрогрессПластик"	по ОКПО	87217275
Идентификационный номер налогоплательщика	ИНН	3123281195
Вид экономической деятельности: организация перевозок грузов	по ОКВЭД	63.4
Организационно-правовая форма/форма собственности: ООО, частная	по ОКОПФ/ОКФС	65 | 16
Единица измерения: тыс. руб. (млн. руб.)	по ОКЕИ	384

Местонахождение (адрес): 308000, г. Белгород, пр-т Б. Хмельницкого, д. 133, оф. 2-36.

Пояснения [1]	Наименование показателя [2]	Код	На 31 декабря 2018 г. [3]	На 31 декабря 2017 г. [4]	На 31 декабря 2016 г. [5]
	АКТИВ				
	I. ВНЕОБОРОТНЫЕ АКТИВЫ				
	Нематериальные активы	1110			
	Результаты исследований и разработок	1120			
	Нематериальные поисковые активы	1130			
	Материальные поисковые активы	1140			
	Основные средства	1150	11350	12618	12036
	Доходные вложения в материальные ценности	1160			
	Финансовые вложения	1170	6551	7544	220
	Отложенные налоговые активы	1180			
	Прочие внеоборотные активы	1190			
	Итого по разделу I	1100	17901	20162	12316
	II. ОБОРОТНЫЕ АКТИВЫ				
	Запасы	1210	14239	13987	5890
	Налог на добавленную стоимость по приобретенным ценностям	1220	103	95	23
	Дебиторская задолженность	1230	7255	13980	8829
	Финансовые вложения (за исключением денежных эквивалентов)	1240			
	Денежные средства и денежные эквиваленты	1250	5430	4971	5763
	Прочие оборотные активы	1260	977	618	217
	Итого по разделу II	1200	28704	33531	20722
	БАЛАНС	1600	**46605**	**53693**	**33038**

Приложение Г

Таблица Г.1 – Расчет показателей финансовой составляющей экономической безопасности предприятия

Показатели финансовой составляющей ЭБП	**Значения показателей**			
	Обозначение	**2016 г**	**2017 г**	**2018 г**
Коэффициент автономии	Ка	0,05	0,057	0,06
Коэффициент обеспеченности собственными средствами	Ксос	- 0,43	- 0,58	- 0,55
Коэффициент абсолютной ликвидности	Кабл	0,001	0,20	0,32
Коэффициент текущей ликвидности	Ктл	0,60	0,71	1,09
Коэффициент быстрой ликвидности	Кб	0,33	0,50	0,69

Таблица Г.2 – Оценка интегрального уровня финансовой составляющей фирмы

Показатель/составляющая экономической безопасности	**Оценка (Оц) в зависимости от степени соответствия нормативу**			
	Обозначение	**Абсолютное (оценка 1)**	**Нейтральное (оценка 0,5)**	**Критическое (оценка 0)**
Коэффициент автономии	Ка	>0,5	0,3-0,5	<0,3
Коэффициент обеспеченности собственными средствами	Ксос	>0,1	0-0,1	<0
Коэффициент абсолютной ликвидности	Кабл	>0,2	0,1-0,2	<0,1
Коэффициент текущей ликвидности	Ктл	1,5-3	1-1,5 или >3	<1
Коэффициент быстрой ликвидности	Кб	>2,9	1,23-2,89	<1,23
Уровень финансовой составляющей	Уфс			

Продолжение приложения Г

Таблица Г.3 – Расчет показателей производственно-сбытовой составляющей экономической безопасности фирмы

Показатели финансовой составляющей ЭБП	**Оценка (Оц) в зависимости от степени соответствия нормативу**			
	Обозначение	**2016 г**	**2017 г**	**2018 г**
Рентабельность продаж	Крп	0,24	0,9	2,1
Рентабельность активов	Кра	0,03	0,002	0,19
Коэффициент соотношения дебиторской и кредиторской задолженностей	Ксдк	0,3	0,4	0,3
Коэффициент оборачиваемости оборотных активов	Кооб	1,00	0,88	0,93

Таблица Г.4 – Оценка производственно-сбытовой составляющей фирмы

Показатель/составляющая экономической безопасности	**Оценка (Оц) в зависимости от степени соответствия нормативу**			
	Обозначение	**Абсолютное (оценка 1)**	**Нейтральное (оценка 0,5)**	**Критическое (оценка 0)**
Рентабельность продаж	Крп	>0,2	0,1-0,2	<0,1
Рентабельность активов	Кра	>0,1	0-0,1.	<0
Коэффициент соотношения дебиторской и кредиторской задолженностей	Ксдк	0,9-1	0,5-0,9 или >1	<0,5
Коэффициент оборачиваемости оборотных активов	Кооб	Тенденция роста показателя	Значение показателя практически не меняется	Тенденция сокращения показателя
Уровень производственно-сбытовой составляющей	Упсс			

Продолжение приложения Г

Таблица Г.5 – Оценка технико-технологической безопасности предприятия

Коэффициент /составляющая экономической безопасности	**Оценка в зависимости от степени соответствия нормативному значению**			
	Обозначение	**Абсолютное (оценка 1)**	**Нейтральное (оценка 0,5)**	**Критическое (оценка 0)**
Обновления основных средств	Коб.	>0,1	0-0,1	0
Фондоотдачи	Кф	Рост в динамике	Значение показателя практически не изменилось	Сокращение значения в динамике
Годности основных средств	Кг	>0,5	0,3-0,5	<0,3
Уровень технико-технологической составляющей	Упсс			

Приложение Д

Таблица Д.1 –Результаты оценки уязвимости информационных активов ООО «Facilicom»

Группа уязвимостей Содержание уязвимости	**Отчеты о деятельность подразделений**	**Сервер с базой электронных писем**	**База данных бухгалтерии**	**Сервер БД с информацией о клиентах**
1. Среда и инфраструктура				
Отсутствие системы контроля доступа сотрудников к чужим АРМ.	низкая	средняя	низкая	средняя
Отсутствие системы видеонаблюдения в организации.	средняя	высокая	средняя	высокая
Несогласованность в системе охраны периметра.	средняя	средняя	средняя	средняя
Отсутствия соглашения о неразглашении между работником и работодателем.	высокая	высокая	высокая	высокая
Нечеткая регламентация ответственности сотрудников организации.	средняя	средняя	высокая	высокая
2. Аппаратное обеспечение				
Неорганизованный контрольно-пропускной режим в организации.	среднее	высокая	средняя	высокая
Отсутствие видеонаблюдения в серверной комнате.	низкая	средняя	низкая	средняя
Отсутствие охранной сигнализации.	низкая	средняя	низкая	средняя
Отсутствие соглашения о нераспространении конфиденциальной информации.	высокая	среднее	высокая	среднее
Нечеткая регламентация ответственности сотрудников организации.	средняя	средняя	средняя	средняя
3. Программное обеспечение				
Неорганизованность контрольно-пропускного пункта.	низкая	низкая	низкая	низкая
Отсутствие системы видеонаблюдения в организации.	средняя	низкая	средняя	низкая
Отсутствие системы охранной сигнализации.	низкая	низкая	низкая	низкая
Отсутствие соглашения о неразглашении конфиденциальной информации.	низкая	низкая	низкая	низкая

Продолжение табл. Д.1

Нечеткое распределение ответственности конфиденциальной информации) между сотрудниками организации.	средняя	низкая	средняя	низкая
Нечеткая организация конфиденциального документооборота в организации.	средняя	низкая	средняя	низкая
Неконтролируемый доступ сотрудников к копировальной и множительной технике	средняя	низкая	средняя	низкая
4. Коммуникации				
Неорганизованный контрольно-пропускной режим в организации. Отсутствие системы видеонаблюдения в организации.	высокая	средняя	высокая	средняя
	средняя	высокая	средняя	высокая
Несогласованность в системе охраны периметра.	высокая	средняя	высокая	средняя
Нечеткая регламентация ответственности сотрудников предприятия.	средняя	высокая	средняя	высокая
Отсутствие ограничения доступа к сетевым устройствам и коммутационному оборудованию, внутренней сети предприятия.	средняя	средняя	средняя	средняя