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

ИНСТИТУТ ЭКОНОМИКИ

КАФЕДРА ЭКОНОМИКИ И МОДЕЛИРОВАНИЯ
ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Выпускная квалификационная работа
обучающегося по специальности 38.05.01 Экономическая безопасность
очной формы обучения, группы 06001310
Тригуб Андрея Алексеевича

Научный руководитель
к.э.н., доцент
Калугин В.А.

Рецензент
Генерального директора
ООО Завод «Энерготехмонтаж»
Гардеев В.Р.

БЕЛГОРОД 2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В последние годы многие российские компании хорошо осознали необходимость управления информационной безопасностью предприятия. Эффективное управление вопросами информационной безопасности приобретает все большее значение для российских компаний по мере их роста и продвижения на новые рынки товаров и услуг. Клиентам важно знать, что соблюдается конфиденциальность их персональных и деловых данных. Инвесторам необходима уверенность в том, что бизнес и информационные активы компании защищены. Деловые партнеры ожидают, что компания будет функционировать без сбоев, которые могут быть вызваны ошибками в работе информационных систем, умышленными или неумышленными действиями персонала, вредоносным программным обеспечением и другими факторами.

На современном этапе состояния общества информационные технологии (ИТ) активно внедряются во все сферы национальной экономики. Сегодня руководство любого промышленного предприятия, по существу, имеет дело с корпоративной информацией, на основе которой оно и принимает решения. Такая информация должна соответствовать требованиям актуальности, достоверности, структурированности, и, если надо, конфиденциальности. Усложнение средств, методов, форм автоматизации процессов обработки информации повышает зависимость промышленных предприятий от степени безопасности используемых ими ИТ, при этом качество информационной поддержки управления напрямую зависит от организации инфраструктуры защиты информации (ИЗИ). Анализ результатов исследований, ведущихся в направлении обеспечения ин- формационной безопасности (ИБ) ИТ показывает, что в настоящее время не до конца решены вопросы научного обоснования структуры системы защиты информации (СЗИ). В первую очередь это касается инфраструктуры защиты бизнес-процессов, которые в свете современных тенденций организации бизнеса играют решающую роль в достижении успеха хозяйствующим субъектом. Отмеченные обстоятельства обуславливают противоречие между необходимостью научного обоснования концепции построения ИЗИ бизнес-процессов и возможностями теоретико-методологических решений, обеспечивающих это обоснование. Процессно-ориентированный подход к созданию (совершенствованию) ИЗИ бизнес-процессов позволит рассматривать процесс формирования СЗИ как один из вспомогательных процессов, обеспечивающих основные процессы предприятия. Это дает возможность разработки ИЗИ в тесной взаимосвязи с проектированием других бизнес-процессов, что увеличит их интегрированность, гибкость, сбалансированность и управляемость.

Таким образом, под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Вопросы безопасности - важная часть концепции внедрения новых информационных технологий во все сферы жизни общества.

Как правило, главными препятствиями на пути обеспечения информационной безопасности являются ее невысокая приоритетность при распределении ресурсов и бюджетные ограничения. Компании нередко выделяют единый бюджет на удовлетворение всех потребностей по информационным системам (аппаратное и программное обеспечение, зарплата, консультанты и т.п.), что способствует развитию тенденции выделять основную часть средств на повышение производительности. При этом нередко вопросы информационной безопасности остаются без внимания.

Выборочная и бессистемная реализация средств безопасности не сможет обеспечить необходимого уровня защиты. Чтобы надежно защитить важнейшую деловую информацию, компаниям необходимо интегрировать вопросы физической и информационной безопасности в единый для всей организации процесс – процесс управления информационной безопасностью предприятия. Обеспечение необходимого уровня информационной безопасности является серьезной проблемой. Это стимулирует развитие различных методологий в данной области, что делает данный вопрос актуальным. Возникает потребность разрабатывать и усовершенствовать корпоративную политику информационной безопасности, в рамках которой предполагается возможность использования распределенной модели использования ресурсов по уровням и группам секретности.

Цель выпускной квалификационной работы состоит в оценке эффективности системы защиты информации на предприятии.

Цель исследования обусловила постановку следующих задач:

- проанализировать сущность, задачи и принципы защиты информации на предприятии;

- охарактеризовать угрозы безопасности информации;

- выявить основные методы, средства и механизмы обеспечения безопасности информации в информационных технологиях;

- дать организационно-экономическую характеристику предприятия;

- проанализировать критерии экономической безопасности предприятия;

- оценить эффективность системы защиты информации на предприятии;

- предложить и экономически обосновать мероприятии по совершенствованию системы защиты информации на предприятии.

Объект выпускной квалификационной работы – ООО «Белгородский завод «Энерготехмонтаж».

Предмет исследования – система защиты информации 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.

При обработке аналитического материала и оформлении работы использовались пакеты прикладных программ Microsoft Excel, Microsoft Word и др.

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. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Содержание и принципы защиты информации на предприятии

Информация – важный ресурс деятельности предприятия. В современном предприятии, наряду с производственной и социальной инфраструктурами следует выделять информационную инфраструктуру, обеспечивающую информационными ресурсами все уровни управления предприятием. Под информационной инфраструктурой следует понимать не только совокупность программно-технических средств и организационно-административных мероприятий, обеспечивающих в совокупности безопасную обработку данных и информационное обеспечение (ИО) бизнес-процессов внутри предприятия, адекватные возможности по обмену информацией с внешними организациями, но и информационные системы и сети, научно- техническое обеспечение, технические библиотеки и саму обрабатываемую информацию. Поддержка и защита системы управления предприятием подразумевает прежде всего поддержку и защиту самих бизнес-процессов и развитие инфраструктурной составляющей бизнес-системы и, в частности, информационной, за счет преодоления инфраструктурной и информационной разобщенности подразделений предприятия. Инвестиции в управление бизнес-процессами могут приносить значительные доходы за счет повышения эффективности работы и ускорения бизнес-процессов, а также за счет повышения рыночной стоимости компании в части ее нематериальных активов: информационных в инфраструктурной составляющей нематериальных активов [23].

Понятие информационных активов следует использовать в широком смысле, включив в него все техническое и программное обеспечение (ПО), патенты, торговые марки и все то, что позволяет работникам предприятия реализовать свой производственный потенциал, а также отношения, сложившиеся между компанией и ее крупными клиентами, государственными структурами, другими хозяйственными объектами. Проведенный анализ возможных угроз показал, что информационная инфраструктура должна обладать свойством защищенности информации, используемой в бизнес-процессах.

С учетом компонентов бизнес-процесса, а также их взаимосвязей, к потенциально опасным ситуациям, которые могут возникнуть при низком уровне защищенности информации, относятся [23]:

– несанкционированный доступ нарушителей (не владельцев и участников) к информации, хранящейся и обрабатываемой в средствах автоматизации, с целью ознакомления, искажения или уничтожения;

– перехват информации при ее приеме (передаче) по каналам связи (сети) функциями процесса, а также за счет хищения носителей информации;

– уничтожение (изменение, искажение) информации за счет случайных помех, сбоев технических (программных) средств при передаче, хранении и обработке информации;

– несанкционированное влияние на бизнес-процесс нарушителей из числа владельцев и (или) участников процесса.

Основные проблемы совершенствования инфраструктуры защиты информации на предприятии представлены на рисунке 1.1.

Обеспечение информационной безопасности является одним из необходимых аспектов ведения бизнеса в условиях агрессивной рыночной экономики.

В современном деловом мире происходит процесс миграции материальных активов в сторону информационных. По мере развития организации усложняется ее информационная система, основной задачей которой является обеспечение максимальной эффективности ведения бизнеса в постоянно меняющихся условиях конкуренции на рынке.

Рис.1.1. Проблемы совершенствования инфраструктуры защиты информации на предприятии [21].

Рассматривая информацию как товар, можно сказать, что информационная безопасность в целом может привести к значительной экономии средств, в то время как ущерб, нанесенный ей, приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и как следствие нарушения информационной безопасности, владелец технологии, а может быть и автор, потеряют часть рынка и т.д. С другой стороны, информация является субъектом управления, и ее изменение может привести к катастрофическим последствиям в объекте управления.

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем (17,28).

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность (17,42):

– целостность данных - защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;

– конфиденциальность информации;

– доступность информации для всех авторизованных пользователей.

Широкое применение компьютерных технологий в автоматизированных системах обработки информации и управления привело к обострению проблемы защиты информации, циркулирующей в компьютерных системах, от несанкционированного доступа.

Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жёстко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно очень большое число угроз информации, которые могут быть реализованы как со стороны внешних нарушителей, так и со стороны внутренних нарушителей.

В области защиты информации и компьютерной безопасности в целом наиболее актуальными являются три группы проблем (14,45):

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение работоспособности информационно-вычислительных систем.

Защита информации превращается в важнейшую проблему государственной безопасности, когда речь идет о государственной, дипломатической, военной, промышленной, медицинской, финансовой и другой доверительной, секретной информации. Огромные массивы такой информации хранятся в электронных архивах, обрабатываются в информационных системах и передаются по телекоммуникационным сетям. Основные свойства этой информации - конфиденциальность и целостность, должны поддерживаться законодательно, юридически, а также организационными, техническими и программными методами.

Конфиденциальность информации (от лат. confidentia - доверие) предполагает введение определенных ограничений на круг лиц, имеющих доступ к данной информации. Степень конфиденциальности выражается некоторой установленной характеристикой (особая важность, совершенно секретно, секретно, для служебного пользования, не для печати и т.п.), которая субъективно определяется владельцем информации в зависимости от содержания сведений, которые не подлежат огласке, предназначены ограниченному кругу лиц, являются секретом. Естественно, установленная степень конфиденциальности информации должна сохраняться при ее обработке в информационных системах и при передаче по телекоммуникационным сетям (13,67).

Другим важным свойством информации является ее целостность (integrty). Информация целостна, если она в любой момент времени правильно (адекватно) отражает свою предметную область. Целостность информации в информационных системах обеспечивается своевременным вводом в нее достоверной (верной) информации, подтверждением истинности информации, защитой от искажений и разрушения (стирания) (13,70).

Несанкционированный доступ к информации лиц, не допущенных к ней, умышленные или неумышленные ошибки операторов, пользователей или программ, неверные изменения информации вследствие сбоев оборудования приводят к нарушению этих важнейших свойств информации и делают ее непригодной и даже опасной. Ее использование может привести к материальному и/или моральному ущербу, поэтому создание системы защиты информации, становится актуальной задачей. Под безопасностью информации понимают защищенность информации от нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Безопасность информации в информационной системе или телекоммуникационной сети обеспечивается способностью этой системы сохранять конфиденциальность информации при ее вводе, выводе, передаче, обработке и хранении, а также противостоять ее разрушению, хищению или искажению. Безопасность информации обеспечивается путем организации допуска к ней, защиты ее от перехвата, искажения и введения ложной информации. С этой целью применяются физические, технические, аппаратные, программно-аппаратные и программные средства защиты. Последние занимают центральное место в системе обеспечения безопасности информации в информационных системах и телекоммуникационных сетях.

Задачи обеспечения безопасности (17,63):

- защита информации в каналах связи и базах данных криптографическими методами;
- подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь);
- обнаружение нарушений целостности объектов данных;
- 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;

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

Построение системы защиты информации связано с формированием принципов, на которых она будет построена. Система защиты информации является сложной системой, выполняющей свою роль в условиях неопределенности, при этом требующая существенных материальных затрат.

Рассмотрим основные принципы построения системы защиты данных (17, 101):

1. Принцип законности

Сущность данного принципа заключается в соблюдении системой основных законов, регламентирующих деятельность по защите информации, а при отсутствии законодательных актов – соблюдении нормативных документов.

2. Принцип полноты информации

Данный принцип основан на защите системой не только информации предприятия, носящей конфиденциальный характер, но и информации, разглашение которой может принести вред данному предприятию. Реализация данного принципа кроме того позволяет обеспечить охрану интеллектуальной собственности на предприятии.

3. Принцип обоснованности защиты информации

При рассмотрении информации предприятия необходимо определить необходимость засекречивания тех или иных данных, при этом защищая интересы государства, общества, граждан, а также рассматриваемого предприятия. Выборочное засекречивание информации позволяет экономить денежные средства от данных манипуляций.

4. Принцип создания специализированных подразделений по защите информации

Комплексная защита информации на предприятии невозможна без создания данного рода службы. К функциям подразделения будет относиться осуществление защитных мероприятий на предприятии, а также осуществление контроля за их выполнением.

5. Принцип участия в защите информации всех соприкасающихся с нею лиц

Данный принцип предполагает, что защита информации работником, имеющем к ней отношение или соприкасающегося с ней, является его служебной обязанностью.

Данные мероприятия способствуют повышению уровня защиты конфиденциальной информации.

6. Принцип персональной ответственности за защиту информации

Каждый работник предприятия, а также лица, соприкасающиеся с конфиденциальной информацией, имеют персональное отношение к ее защите и неразглашении. Данные лица несут уголовную, административную и иные виды ответственности за нарушение конфиденциальности данной информации.

7. Принцип наличия и использования всех необходимых правил и средств для защиты

Заключается в том, что система защиты информации требует, с одной стороны, участия в ней руководства предприятия и специальной службы защиты информации и всех исполнителей, работающих с защищаемой информацией, с другой стороны, использования различных организационных форм и методов защиты, с третьей стороны, наличие необходимых материально-технических ресурсов, включая технические средства защиты.

8. Принцип превентивности принимаемых мер по защите информации

Предполагает априорное опережающее заблаговременное принятие мер по защите до начала разработки или получения информации. Из этого принципа вытекает, в частности, необходимость разработки защищенных информационных технологий.

1.2. Классификация угроз безопасности информации

Информация как объект защиты имеет множество определений, например, в ФЗ РФ «Об информации, информационных технологиях и о защите информации» (от 2006г.) принято определение: Информация – сведения о лицах, предметах, фактах и процессах независимо от формы их представления.

С точки зрения информационной безопасности считается, что информация должна обладать 5 категориями (20,92):

1. Доступность (гарантия того, что авторизованный пользователь мог бы получить доступ к соответствующей информации);

2. Целостность (гарантия сохранения за информацией правильных значений, не измененных в процессе хранения и передачи);

3. Конфиденциальность (гарантия того, что информация доступна только тем пользователям, которым этот доступ разрешен);

4. Аутентичность (гарантия того, что автором информации является то лицо, которое заявлено ее автором);

5. Аппилируемость (гарантия того, что автором информационного сообщения является именно заявленное лицо и никто иной).

Защищенная система – система, удовлетворяющая требованиям безопасности, использующих ее субъектов информационных отношений, в которых возможные риски сведены к минимуму.

Защищенность – качественная характеристика систем и обычно измеряется комплексом показателей или характеристик.

Для каждого отдельного случая понятие защищенности системы может быть различным.

Угроза – опасность (существующая реально или потенциально) совершения какого-либо деяния, направленного на нарушение основных свойств информации (доступность, целостность, конфиденциальность).

Основные причины возникновения угроз:

- технологические (недостатки ОС, стека протоколов TCP/IP и сетевого оборудования);

- недостатки конфигурации (неправильные настройки сетевого оборудования и служб Internet);

- недостатки политики безопасности (отсутствие документированных правил, небрежность администрирования и контроля, частая смена персонала).

Рассмотрим классификацию угроз безопасности информации в информационных технологиях (20,110):

1. По мотивации: умышленные и неумышленные;

2. По видам нарушителей:

- Внутренние (служащие с враждебными намерениями; служащие совершающие непреднамеренные нарушения);

- Внешние (любители острых ощущений; конкуренты; похитители; враждебно настроенные бывшие сотрудники).

3. По видам вредносного ПО:

- Вирус – небольшая программа, которая создана для изменения информации без ведома пользователя;

- Троян – вредоносная программа, которая содержится внутри другой безвредной программы, выполняет роль шпиона (перехват и передача важной информации третьим лицам) и запускается пользователем;

- Червь – вредоносная программа, которая самостоятельно распространяет свои копии по локальной и по глобальной сети.

Субъекты, реализующие угрозы безпасности информации в информационных технологиях, называются нарушителями.

Рассмотрим предполагаемые категории нарушителей на рис. 1.2.

Основными мотивами нарушителей являются:

- безответственность;

- самоутверждение;

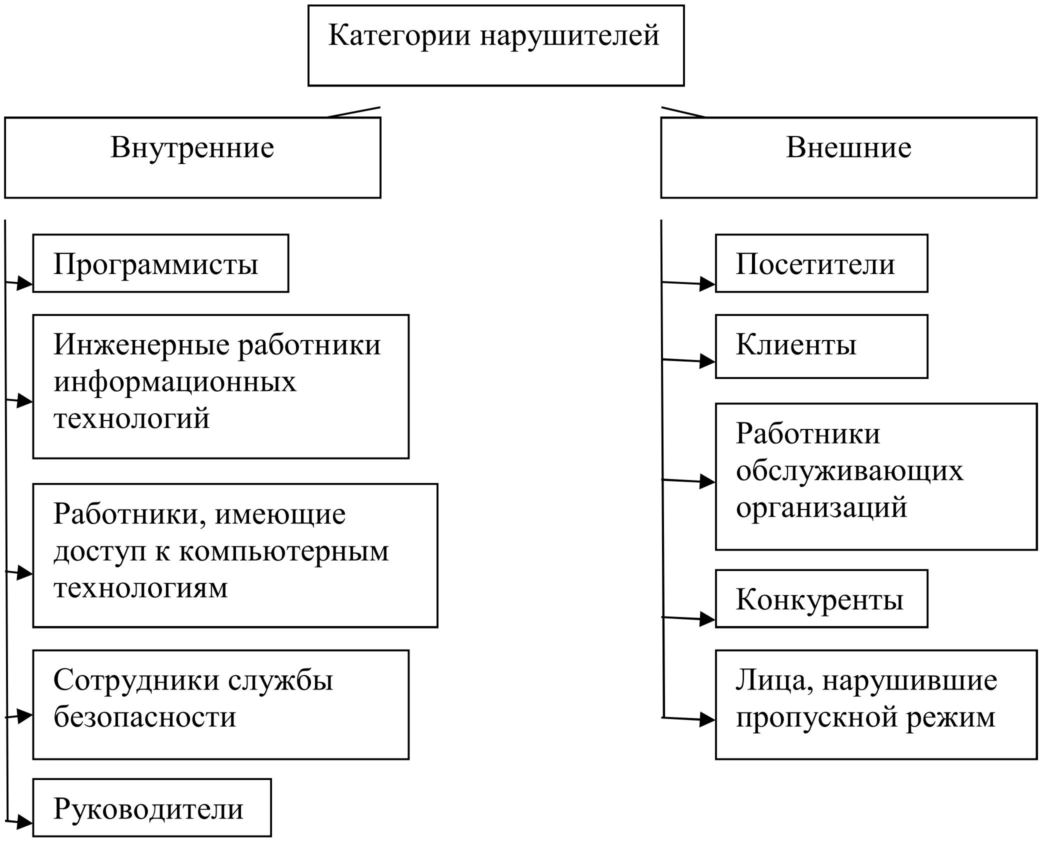


Рис. 1.2. Предполагаемые категории нарушителей (20)

- корыстный интерес.

Рассмотрим основную классификацию нарушителей в таблице 1.1.

Таблица 1.1

Классификация нарушителей

Классификационный признак	Виды нарушителей
1	2
По уровню знаний информационных технологий	знающих функциональные особенности информационной технологии, умеющих пользоваться штатными средствами
	обладающих высоким уровнем знаний и опытом работы с техническими средствами информационной технологии и их обслуживания
	обладающих высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации информационных технологий
	знающих структуру, функции и механизм действия средств защиты, их сильные и слабые стороны

Продолжение табл. 1.1

1	2
По уровню возможностей	применяющие агентурные методы получения сведений
	применяющие пассивные средства (технические средства перехвата без модификации компонентов информационной технологии)
	использующие только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные машинные носители информации, которые могут быть скрытно пронесены через посты охраны
	применяющие методы и средства активного воздействия (модификация и подключение дополнительных устройств, внедрение программных «закладок» и т. д.)
По времени действия	в процессе функционирования информационной технологии (во время работы компонентов системы)
	в нерабочее время, во время плановых перерывов в работе информационной технологии, перерывов для обслуживания и ремонта и т. д.
	как в процессе функционирования информационной технологии, так и в нерабочее время
По месту действия	имеющие доступ в зону управления средствами обеспечения безопасности ИТ
	имеющие доступ в зону данных
	действующие с автоматизированных рабочих мест (рабочих станций)
	действующие внутри помещений, но не имеющие доступа к техническим средствам информационной технологии
	действующие с контролируемой территории без доступа в здания и сооружения
	не имеющие доступа на контролируемую территорию организации

Определение конкретных значений характеристик потенциальных нарушителей в значительной степени субъективно. Поэтому все выше указанные характеристики рассматриваются в комплексе с учетом тщательной проверки каждой.

1.3. Способы защиты информации информации на предприятии

Технологии защиты данных основываются на применении современных методов, которые предотвращают утечку информации и ее потерю. Сегодня используется шесть основных способов защиты (рис. 1.3):

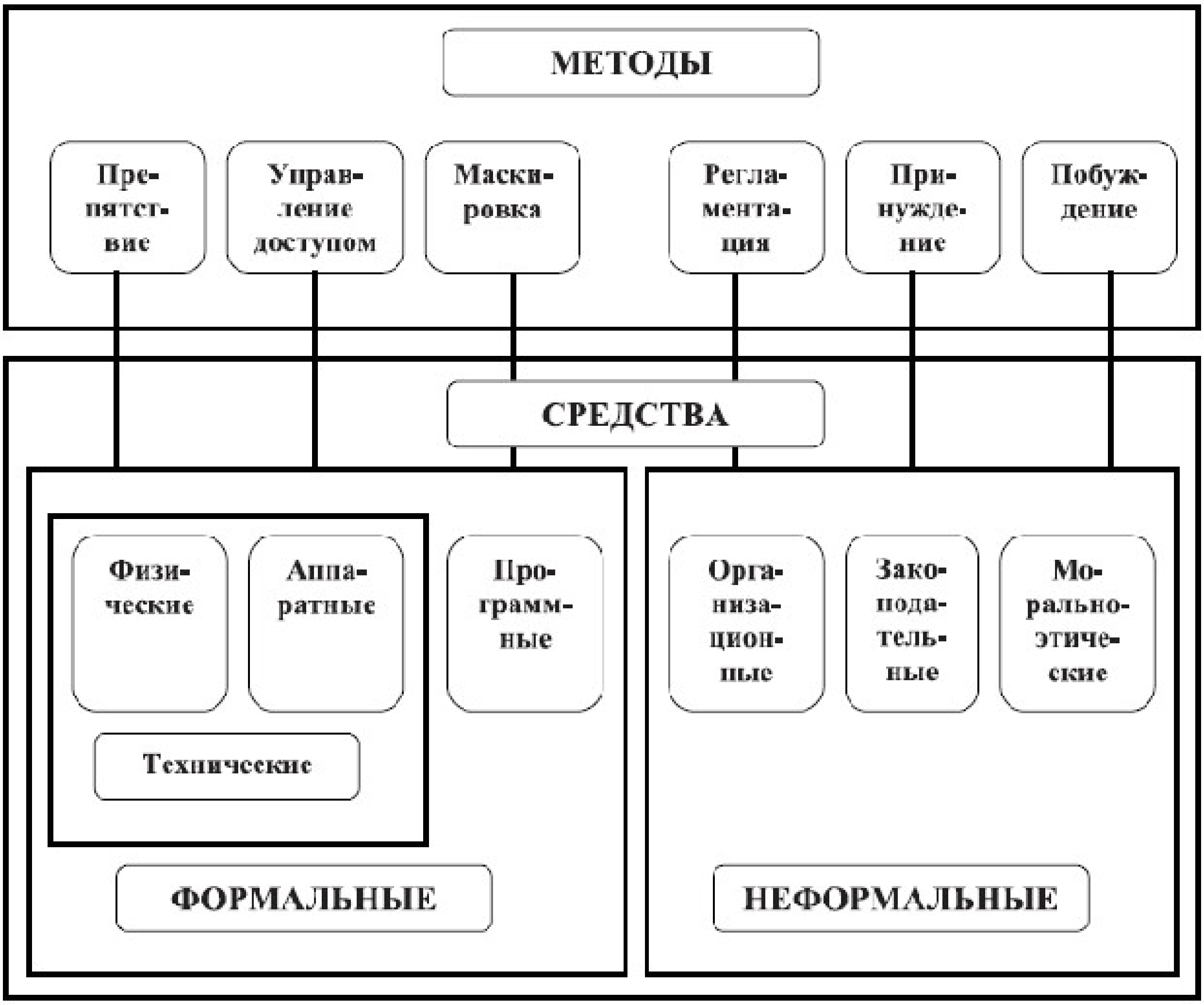


Рис. 1.3. Методы обеспечения безопасности информации (29)

Все перечисленные методы нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

Под препятствием понимается способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию.

Маскировка - способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа (29).

Управление - способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.

Регламентация - важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение - методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении.

Способы защиты информации предполагают использование определенного набора средств. Для предотвращения потери и утечки секретных сведений используются следующие средства (33):

1. Физические;
2. Программные и аппаратные;
3. Организационные;
4. Законодательные;
5. Психологические.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных как на бумажных, так и на электронных носителях.

Программные и аппаратные средства - незаменимый компонент для обеспечения безопасности современных информационных систем. Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации.

Программные средства - программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации - для предотвращения потерь.

Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Законодательные средства - комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.

Психологические средства - комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.

Для обеспечения безопасности информационных систем сегодня активно используются методы шифрования и защиты электронных документов. Данные технологии позволяют осуществлять удаленную передачу данных и удаленное подтверждение подлинности.

Методы защиты информации путем шифрования (криптографические) основаны на изменении информации с помощью секретных ключей особого вида. В основе технологии криптографии электронных данных - алгоритмы преобразования, методы замены, алгебра матриц. Стойкость шифрования зависит от того, насколько сложным был алгоритм преобразования. Зашифрованные сведения надежно защищены от любых угроз, кроме физических (29).

Электронная цифровая подпись (ЭЦП) - параметр электронного документа, служащий для подтверждения его подлинности. Электронная цифровая подпись заменяет подпись должностного лица на бумажном документе и имеет ту же юридическую силу. ЭЦП служит для идентификации ее владельца и для подтверждения отсутствия несанкционированных преобразований. Использование ЭЦП обеспечивает не только защиту информации, но также способствует удешевлению технологии документооборота, снижает время движения документов при оформлении отчетов.

Используемая технология защиты и степень ее эффективности определяют класс безопасности информационной системы. В международных стандартах выделяют 7 классов безопасности систем, которые объединены в 4 уровня (33):

- D - нулевой уровень безопасности;
- C - системы с произвольным доступом;
- B - системы с принудительным доступом;

- А - системы с верифицируемой безопасностью.

Уровню D соответствуют системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям. Использование слаборазвитой технологии защиты чревато потерей или утратой сведений. В уровне С есть следующие классы — С1 и С2.

Класс безопасности С1 предполагает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности С1 в системе имеются аппаратные и программные средства защиты. Системы с классом С2 дополнены мерами, гарантирующими ответственность пользователей: создается и поддерживается журнал регистрации доступа. Уровень В включает технологии обеспечения безопасности, которые имеют классы уровня С, плюс несколько дополнительных.

Класс В1 предполагает наличие политики безопасности, доверенной вычислительной базы для управления метками безопасности и принудительного управления доступом. При классе В1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности В2 характерен для многих современных систем и предполагает (39):

- снабжение метками секретности всех ресурсов системы;
- регистрацию событий, которые связаны с организацией тайных каналов обмена памятью;
- структурирование доверенной вычислительной базы на хорошо определенные модули;
- формальную политику безопасности;
- высокую устойчивость систем к внешним атакам.

Класс B3 предполагает, в дополнение к классу B1, оповещение администратора о попытках нарушения политики безопасности, анализ появления тайных каналов, наличие механизмов для восстановления данных после сбоя в работе аппаратуры или программного обеспечения. Уровень A включает один, наивысший класс безопасности — A. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям верхнего уровня.

Организация защиты ресурсов информационной технологии от компьютерных вирусов выглядит следующим образом. Под понятием «вредоносного программного обеспечения» подразумевается любая программа, созданная и используемая для осуществления несанкционированных и часто вредоносных действий. Как правило, к нему относят разного рода вирусы, черви, троянцы, клавиатурные шпионы, программы для кражи паролей, макровирусы, вирусы сектора загрузки, скриптовые вирусы, мошенническое ПО, шпионские и рекламные программы. К сожалению, этот далеко неполный список, который с каждым годом пополняется все новыми и новыми видами вредоносных программ, которые в данном материале мы часто будем называть общим словом - вирусы.

Мотивы написания компьютерных вирусов могут быть самыми разными: от банального желания проверить свои силы в программировании до желания навредить или получить незаконные доходы.

Например, некоторые вирусы не приносят почти никакого вреда, а только замедляют работу машины за счет своего размножения, замусоривая при этом, жесткий диск компьютера или производят графические, звуковые и другие эффекты. Иные же могут быть очень опасными, приводя к потере программ и данных, стиранию информации в системных областях памяти и даже к выходу из строя частей жесткого диска.

Рассмотрим основные виды вирусов на рис. 1.4.

Рис. 1.4. Основные виды вирусов (39)

Одна из первостепенных задач злоумышленников – найти способ доставки зараженного файла на компьютер и заставить его там активироваться. Источники заражения компьютерными вирусами приведены на рис. 1.5.

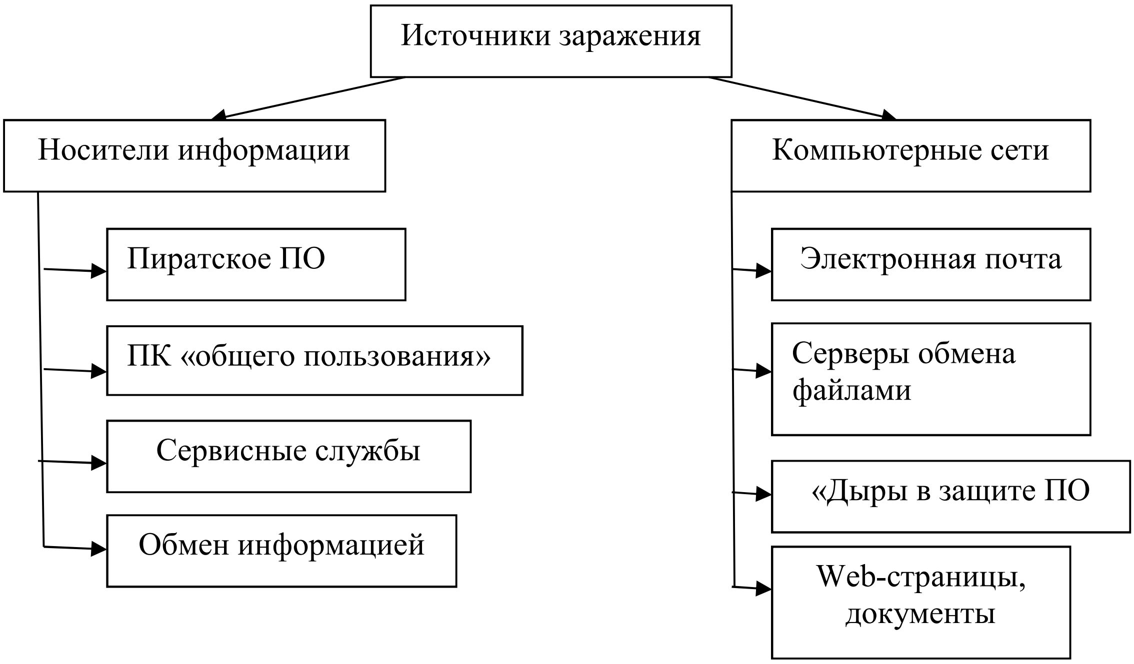


Рис. 1.5. Источники заражения (39)

На сегодняшний день основным источником вирусов является всемирная глобальная сеть. С какими же видами компьютерных угроз может столкнуться любой рядовой пользователь глобальной сети интернет (33):

1. Кибервандализм. Распространение вредоносного ПО с целью повреждения данных пользователя и вывода компьютера из строя [40].

2. Мошенничество. Распространение вредоносного ПО для получения незаконных доходов. Большинство программ используемых с этой целью позволяют злоумышленникам собирать конфиденциальную информацию и использовать ее для кражи денег у пользователей.

3. Хакерские атаки. Взлом отдельных компьютеров или целых компьютерных сетей с целью кражи конфиденциальных данных или установки вредоносных программ.

4. Фишинг. Создание подложных сайтов, которые являются точной копией существующих (например, сайта банка) с целью кражи конфиденциальных данных при их посещении пользователями.

5. Спам. Анонимные массовые рассылки электронной почты, которые засоряют электронные ящики пользователей. Как правило, используются для рекламы товаров и услуг, а так же фишинговых атак.

6. Рекламное программное обеспечение. Распространение вредоносного ПО, запускающего рекламу на вашем компьютере или перенаправляющего поисковые запросы на платные (часто порнографические) веб-сайты. Нередко бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя без его ведома.

7. Ботнеты. Зомби-сети, состоящие из зараженных с помощью троянца компьютеров (среди которых может быть и ваш ПК), управляемых одним хозяином и используемых для его целей (например, для рассылки спама).

Для обнаружения и обезвреживания вирусов применяются специальные программы, которые так и называются «антивирусные программы» или «антивирусы». Они блокируют несанкционированный доступ к вашей информации извне, предотвращают заражение компьютерными вирусами и в случае необходимости, ликвидируют последствия заражения.

В настоящее время используют следующие технологии антивирусной защиты. Наличие той или иной технологии в составе антивирусного пакета, зависит от того, как позиционируется продукт на рынке и влияет на его конечную стоимость (29):

1. Файловый антивирус. Компонент, контролирующий файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на компьютере. В случае обнаружения известных вирусов, как правило, предлагается вылечить файл. Если по каким-то причинам это невозможно, то он удаляется или перемещается на карантин.

2. Почтовый антивирус. Обеспечивает защиту входящей и исходящей почты и осуществляет ее проверку на наличие опасных объектов.

3. Вэб антивирус. Осуществляет антивирусную проверку трафика, передающегося по интернет протоколу HTTP, что обеспечивает защиту вашего браузера. Контролирует все запускающиеся скрипты на предмет вредоносного кода, включая Java-scriptи VB-script.

4. IM-антивирус. Отвечает за безопасность работы с интернет-пейджерами (ICQ, MSN, Jabber, QIP, Mail.RUАгент и т. д.) проверяет и защищает информацию, поступающую по их протоколам [40].

5. Контроль программ. Этот компонент регистрирует действия программ, запущенных в операционной системе, и регулирует их деятельность на основе установленных правил. Эти правила регламентируют доступ программ к различным ресурсам системы.

6. Сетевой экран (брандмауэр). Обеспечивает безопасность работы в локальных сетях и интернет, отслеживания во входящем трафике активность,

характерную для сетевых атак, использующих уязвимости операционных систем и программного обеспечения. Ко всем сетевым соединениям применяются правила, которые разрешают или запрещают те или иные действия на основании анализа определенных параметров.

7. Проактивная защита. Этот компонент призван выявлять опасное программное обеспечение на основе анализа его поведения в системе. К вредоносному поведению может относиться: активность, характерная для троянских программ, доступ к реестру системы, самокопирование программ в различные области файловой системы, перехват ввода данных с клавиатуры, внедрение в другие процессы и т. д. Таким образом осуществляется попытка защитить компьютер не только от уже известных вирусов, но и от новых, еще не исследованных.

8. Анти-Спам. Фильтрует всю входящую и исходящую почту на предмет нежелательных писем (спама) и сортирует ее в зависимости от настроек пользователя.

9. Анти-Шпион. Важнейший компонент, призванный бороться с мошенничеством в сети интернет. Защищает от фишинг-атак, «бэкдор»-программ, загрузчиков, уязвимостей, взломщиков паролей, захватчиков данных, перехватчиков клавиатуры и прокси-серверов, программ автоматического дозвона на платные вэб-сайты, программ-шуток, программ-реклам и назойливых баннеров.

10. Родительский контроль. Это компонент, позволяющий установить ограничения доступа использования компьютера и интернета. С помощью этого инструмента вы сможете контролировать запуск различных программ, использование интернета, посещение вэб-сайтов в зависимости от их содержимого и многое другое, тем самым ограждая детей и подростков от негативного влияния при работе на компьютере.

11. Безопасная среда или песочница (Sandbox). Ограниченное виртуальное пространство, перекрывающее доступ к ресурсам системы. Обеспечивает

защищенную работу с приложениями, документами, интернет-ресурсами, а также с веб-ресурсами интернет-банкинга, где особое значение имеет безопасность при вводе конфиденциальных данных. Так же позволяет внутри себя запускать небезопасные приложения без риска заражения системы.

Универсального способа борьбы с вирусами не существует. Даже если на компьютере стоит самая современная антивирусная программа – это абсолютно не гарантирует тот факт, что ваша система не будет заражена. Ведь сначала появляются вирусы, а лишь потом только лекарство от них. И не смотря на то, что многие современные антивирусные решения имеют системы обнаружения еще неизвестных угроз, их алгоритмы несовершенны и не обеспечивают вам 100% защиту. Но, если придерживаться основных правил антивирусной защиты, то есть возможность существенно снизить риск заражения компьютера и утраты важной информации (27,129):

- установка хорошей антивирусной программы;
- резервное копирование ценных данных;
- разбивка жесткого диска на несколько разделов;
- ограничение посещений сайтов сомнительного происхождения;
- ограничение сомнительных почтовых рассылок;
- ограничение пользования социальными сетями.

Таким образом, актуальность проблемы защиты информации сегодня не вызывает сомнений. Успех современной компании и ее развитие в условиях острой конкуренции в значительной степени зависят от применения информационных технологий, а следовательно, от степени обеспечения информационной безопасности.

Любое предприятие располагает различными видами информации, представляющими интерес для злоумышленников. Прежде всего, это коммерческие данные, информация, являющаяся интеллектуальной собственностью предприятия и конфиденциальные данные.

Поэтому защите информации от неправомерного овладения ею отводится весьма значительное место. При этом целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Как видно из этого определения целей защиты, информационная безопасность - довольно емкая и многогранная проблема, охватывающая не только определение необходимости защиты информации, но и то, как ее защищать, от чего защищать, когда защищать, чем защищать и какой должна быть эта защита.

Для того чтобы отразить подход организации к защите своих информационных активов необходимо разработать политику информационной безопасности. Каждое предприятие должно осознать необходимость поддержания соответствующего режима безопасности и выделения на эти цели значительных ресурсов.

ГЛАВА 2. АНАЛИЗ ОСНОВНЫХ КРИТЕРИЕВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ООО «БЕЛГОРОДСКИЙ ЗАВОД «ЭНЕРГОТЕХМОНТАЖ»

2.1. Организационно-экономическая характеристика предприятия

Предприятие является разработчиком и производителем широкой номенклатуры высоковольтного и низковольтного оборудования. Вся номенклатура выпускаемой продукции имеет сертификаты соответствия качеству.

ООО «Белгородский завод «Энерготехмонтаж» находится по адресу: 308017 г. Белгород, ул. Константина Заслонова, 175-а.

В перспективе планируется расширение производства путем внедрения оборудования на электрогазовом выключателе, организации отдельного структурного подразделения для проведения электромонтажных работ в полном объеме: электротехническая лаборатория, организация пуско-наладочных работ и пр. Ведется работа по организации участка для гальванической обработки металла и участка аргонно-дуговой сварки для работы с электрошиной.

На сегодняшний день потребителями продукции являются предприятия Москвы, Московской области, Ярославля, Уфы, Орла, Воронежа, Волгограда и других регионов Российской Федерации. Предприятие занимается выпуском продукции для строительства трансформаторных подстанций.

Основные виды продукции, занимающие в структуре более 90 %:

- комплектные трансформаторные подстанции (КТП);
- комплектные двухтрансформаторные подстанции наружной установки (2КТП);

вакуумные выключатели;

- трансформаторы.

Организационная структура предприятия относится к наиболее распространенному линейно-функциональному построению организации, традиционно используемым многими предприятиями разных отраслей народного хозяйства. Линейное управление предполагает распределение должностных обязанностей таким образом, чтобы каждый служащий был максимально нацелен на выполнение производственных задач предприятия. В числе преимуществ линейной организации – ответственность, установленные обязательства, четкое распределение обязанностей и полномочий; оперативный процесс принятия решений; проекта в понимании и использовании, возможность поддерживать необходимую дисциплину.

Преимущественно линейны полномочия позволили сформировать стабильную и прочную организацию.

В числе недостатков линейного построении предприятия – негибкость, жесткость, неприспособленность к дальнейшему росту организации, что и будет подтверждено в ходе дальнейшего анализа.

Линейное управление подкрепляется специальными функциональными вспомогательными службами, созданными на ресурсной основе (отдел кадров, бухгалтерия, планово-финансовый отдел, отдел логистики, отдел сертификации продукции). Среди недостатков линейно - функционального построения – разногласия между линейными и функциональными служащими.

Линейные служащий часто противодействуют работе функциональных экспертов; возникающие разногласия выражаются в неправильном толковании полученной от экспертов информации, которая передается линейными служащими непосредственным исполнителям. Имеет место недостаточная компетентность отдельных руководителей, келейность при принятии решений, кастовый подбор кадров. Линейные полномочия снижают эффективность управления у руководителей в силу большой перегрузки информацией, огромного потока документации, множественность контактов с подчиненными. При такой структурной организации системы управления в ООО «Белгородский завод «Энерготехмонтаж»» возможности руководства по рационализации логистической системы крайне ограничены.

Необходимо усиление уровня функционального управления логистической деятельности компании с выделением в ее структуре соответствующего подразделения. В таблице 2.1 представлены основные технико-экономические показатели работы предприятия за 2015-2017 годы.

Таблица 2.1

Основные технико-экономические показатели работы предприятия за 2015 - 2017 годы

Показатели	2015 г.	2016 г.	2017 г.	Абсолютное отклонение (+;-)		Относительное отклонение (%)	
				2016 к 2015	2017 к 2016	2016 к 2015	2017 к 2016
Чистые активы, т.р.	4 203	-16 403	1 345	-20 606	-2 858	-490,27	-68
Оборачиваемость чистых активов, %	46 119,22	-11 689,98	151 781,71	-57 809,21	105 662,49	-125,35	229,11
Рентабельность чистых активов, %	665,76	-326,92	3 160,45	-992,68	2 494,68	-149,10	374,71
Собственный капитал, т.р.	4 203	-16 403	1 345	-20 606	-2 858	-490,27	-68
Рентабельность собственного капитала, %	-601,95	337,80	639,80	939,75	1 241,75	156,12	206,29
Кредиты и займы, т.р.	453 693	462 820	449 635	9 127	-4 058	2,01	-0,89

Динамика чистых активов, собственного капитала и кредитов и займов приведена на рисунке 2.1. Рассматривая динамику показателей финансово – хозяйственной деятельности ООО «Белгородский завод «Энерготехмонтаж»» особое внимание следует обратить на рентабельность чистых активов и средневзвешенную стоимость капитала. Для успешного развития деятельности необходимо, чтобы рентабельность чистых активов была выше средневзвешенной стоимости капитала, тогда предприятие способно выплатить не только проценты по кредитам и объявленные дивиденды, но и реинвестировать части чистой прибыли в производство.

Рис. 2.1. Динамика чистых активов, собственного капитала и кредитов и займов

В таблице 2.2 приведен анализ изменения прибыли предприятия.

Таблица 2.2

Анализ изменения прибыли предприятия, тыс. руб.

Показатели	2015 г.	2016 г.	2017 г.	Абсолютное отклонение (+;-)		Относительное отклонение (%)	
				2016 к 2015	2017 к 2016	2016 к 2015	2017 к 2016
1	2	3	4	5	6	7	8
Выручка	1 938 391	1 917 508	2 041 464	-20 883	103 073	-1,08	5,32

Себестоимость продаж	1 563 601	1 532 602	1 666 563	-30 999	102 962	-1,98	6,58
Валовая прибыль (убыток)	374 790	384 906	374 901	10 116	111	2,70	0,03
Коммерческие расходы	346 394	330 759	331 929	-15 635	-14 465	-4,51	-4,18
Управленческие расходы	414	523	464	109	50	26,33	12,08

Продолжение таблицы 2.2

1	2	3	4	5	6	7	8
Прибыль (убыток) от продаж	27 982	53 624	42 508	25 642	14 526	91,64	51,91
Проценты к получению	3 177	1 608	194	-1 569	-2 983	-49,39	-93,89
Проценты к уплате	31 658	34 741	35 605	3 083	3 947	9,74	12,47
Прочие доходы	88 500	108 861	135 389	20 361	46 889	23,01	52,98
Прочие расходы	113 072	145 816	122 492	32 744	9 420	28,96	8,33
Прибыль (убыток) до налогообложения	-25 071	-16 464	19 994	8 607	45 065	-34,33	-179,75
Чистая прибыль (убыток) отчетного периода	-25 300	-20 606	17 748	4 694	43 048	-18,55	-170,15

Из таблицы 2.1 видно что, на конец анализируемого периода рентабельность собственного капитала составила 639,8%, что выше показателя средневзвешенной стоимости капитала, значение которого составило в соответствующем периоде нулевую величину. Сложившаяся ситуация говорит о том, что предприятие способно выплатить не только проценты по кредитам и объявленные дивиденды, но и реинвестировать часть чистой прибыли в производство.

Рассматривая динамику доходов и расходов ООО «Белгородский завод «Энерготехмонтаж»» можно сказать, что в целом за анализируемый период ее можно назвать положительной.

Из таблицы 2.2 видно, что выручка от реализации компании по сравнению с базовым периодом увеличилась (с 1 938 391 тыс. руб. на 31.12.2015 г. до 2 041 464 тыс. руб. на 31.12.2017 г.). За анализируемый период изменение объема продаж составило 103 073 тыс. руб. Темп прироста составил 5,32%.

Валовая прибыль на 31.12.2015 г. составляла 374 790 тыс. руб. За анализируемый период она возросла на 111 тыс. руб. что следует рассматривать как положительный момент и на 31.12.2017 г. составила 374 901 тыс. руб.

Прибыль от продаж на 31.12.2015 г. составляла 27 982 тыс. руб. За анализируемый период она, так же как и валовая прибыль, возросла на 14 526 тыс. руб., и на 31.12.2017 г. Прибыль от продаж составила 42 508 тыс. руб., также как и валовая прибыль, осталась на прежнем уровне.

Следует отметить высокий уровень коммерческих и управленческих расходов в структуре отчета о прибылях и убытках организации. На начало анализируемого периода их доля составляла 22,18 %, от себестоимости реализованной продукции, а на конец периода – 19,94 % от себестоимости проданных товаров, продукции, работ, услуг.

Показателем снижения эффективности деятельности предприятия можно назвать более высокий рост себестоимости по отношению к росту выручки. Рост себестоимости, в то время как выручка выросла на (5,32 %) составил 6,58 %).

Отрицательным моментом является наличие убытков по прочим доходам и расходам. На 31.12.2017 г. сальдо по ним установилось на уровне -22 514 тыс. руб., однако наблюдается положительная тенденция – за период с конца 31.12.2015 г. по конец 31.12.2017 г. сальдо по прочим доходам и расходам увеличилось на 38 433 тыс. руб.

Чистая прибыль за анализируемый период выросла на 43 048 тыс. руб., и на конец 31.12.2017 г. установилась на уровне 17 748 тыс. руб. (темп прироста составил -170,15%).

2.2. Анализ показателей финансово-хозяйственной деятельности предприятия

Оценив показатели, характеризующие экономическую безопасность предприятия. Для этого определим 3 группы показателей: финансовые, производственные и социальные показатели.

Финансовое состояние предприятия в значительной степени зависит от целесообразности и правильности вложения финансовых ресурсов в активы. Характеристику качественных изменений в структуре средств и их источников можно получить с помощью вертикального и горизонтального анализа отчетности.

На стадии вертикального и горизонтального анализа проводиться оценка деятельности предприятия ООО «Белгородский завод «Энерготехмонтаж»», выявляются изменения в составе его имущества и источниках, устанавливаются взаимосвязи различных показателей.

Экономический анализ финансово-хозяйственной деятельности начинается с оценки финансового состояния по данным бухгалтерского баланса (форма № 1). В таблице 2.3 представление изменение структуры актива бухгалтерского баланса предприятия.

Таблица 2.3

Изменение структуры актива бухгалтерского баланса предприятия, %

Показатели, %	2015 г. тыс. руб.	2016 г. тыс. руб.	2017 г. тыс. руб.	Отклонение (+;-)	
				2016 / 2015	2017 / 2016
Основные средства	3,36	5,03	6,59	1,67	3,23
Прочие вне оборотные активы	0,66	0,46	0,42	-0,2	-0,24
Итого по разделу I	4,03	5,49	7,01	1,46	2,98
Запасы	26,31	35,48	34,25	9,17	4,94
Налог на добавленную стоимость по приобретенным ценностям	0,04	0,02	0,01	-0,02	-0,03
Дебиторская задолженность	59,88	55,73	53,81	-4,15	-6,07
Финансовые вложения	6,67	-	-	-	-
Денежные средства	1,95	1,45	1,07	-0,5	-0,88
Прочие оборотные активы	1,12	1,83	3,85	0,71	2,73
Итого по разделу II	95,97	94,51	92,99	-1,46	-2,98
Баланс	100	100	100	-	-

В таблице 2.4 представлено изменение структуры актива бухгалтерского баланса предприятия.

Таблица 2.4

Изменение структуры пассива бухгалтерского баланса предприятия, %

Показатели, %	2015 г. тыс. руб.	2016 г. тыс. руб.	2017 г. тыс. руб.	Отклонение (+;-)	
				2016 / 2015	2017 / 2016
Уставный капитал	0,1	0 ,1	0,1	-	-

Нераспределенная прибыль (непокрытый убыток)	0,66	-2,91	0,12	-3,57	-0,54
Итого по разделу III	0,76	- 3,01	0,22	-3,77	-0,54
Заемные средства	8,08	7,81	10,25	-0,27	2,17
Итого по разделу IV	8,08	7,81	10,25	-0,27	2,17
Заемные средства	74,22	76,99	64,41	2,77	-9,81
Кредиторская задолженность	16,94	18,21	25,12	1,27	8,18
Итого по разделу V	91,16	95,19	89,53	4,03	-1,63
Баланс	100	100	100	-	-

В таблице 2.5 представлен баланс основных статей бухгалтерского баланса за 2015 – 2017 годы.

Таблица 2.5

Анализ основных статей бухгалтерского баланса за 2015 – 2017 годы

Показатель	2015 г. тыс. руб.	2016 г. тыс. руб.	2017 г. тыс. руб.	Абсолютное отклонение (+;-)		Относительное отклонение (%)	
				2016/ 2015	2017/ 2016	2017/ 2015	2017/ 2016
1	2	3	4	5	6	7	8
Вне оборотные активы	22190	29939	42236	7749	20046	34,92	90,34
Оборотные активы	529094	515838	560026	-13256	30932	-2,51	5,85
Запасы и затраты	145251	193768	206334	48517	61083	33,4	42,05

Продолжение таблицы 2.5

1	2	3	4	5	6	7	8
Краткосрочная дебиторская задолженность	330114	304182	324052	-25932	-6062	- 7,86	-1,84
Денежные	47549	7915	6456	-39634	-41093	-	-86,42

средства и краткосрочные финансовые вложения						83,35	
Прочие оборотные активы.	6180	9973	23184	3793	17004	61,38	275,15
Собственный капитал	4203	-16403	1345	-20606	-2858	-490,27	-68
Долгосрочные пассивы	44538	42637	61723	-1901	17185	-4,27	38,59
Займы и кредиты	44538	42637	61723	-1901	17185	- 4,27	38,59
Краткосрочные пассивы	502543	519543	539194	17000	36651	3,38	7,29
Займы и кредиты	409155	420183	387912	11028	-21243	2,7	-5,19
Кредиторская задолженность	93388	99360	151282	5972	57894	6,39	61,99
Баланс	551284	545777	602262	-5507	50978	- 1	9,25

Анализируя актив баланса видно, что общая величина активов предприятия в отчетном периоде, по сравнению с базовым незначительно увеличилась. По сравнению с концом (31.12.2015 г.) активы и валюта баланса выросли. Таким образом, в отчетном периоде актив баланса и валюта баланса находятся на уровне 602 262 тыс. руб. В более значительной степени это произошло за счет увеличения статьи «запасы». За прошедший период рост этой статьи составил 61 258 тыс. руб. и уже на конец анализируемого периода значение статьи «запасы» достигло 206 289 тыс. руб.

В общей структуре активов вне оборотные активы, величина которых на 31.12.2015 г. составляла 22 190 тыс. руб., возросли на 20 046 тыс. руб. (темп прироста составил 90,34%), и на 31.12.2017 г. их величина составила 42 236 тыс. руб. (7% от общей структуры имущества). Величина оборотных активов, составлявшая на 31.12.2015 г. 529 094 тыс. руб. также возросла на 30932 тыс. руб. (темп прироста составил 5,85%), и на 31.12.2017 г. их величина составила 560 026 тыс. руб. (93% от общей структуры имущества).

Как видно из таблицы 2.5, на конец отчетного периода наибольший удельный вес в структуре совокупных активов приходится на оборотные активы (92,99%), что говорит о достаточно мобильной структуре активов, способствующей ускорению оборачиваемости средств предприятия. К тому же наблюдается положительная тенденция к росту оборотных активов.

В структуре вне оборотных активов наибольшее изменение было вызвано увеличением на 21 151 тыс. руб., по сравнению с базовым периодом, статьи «основные средства»

В структуре оборотных активов наибольшее изменение было вызвано увеличением на 61 258 тыс. руб., по сравнение базовым периодом, статьи «запасы».

Размер дебиторской задолженности за анализируемый период в сумме снизился на 6 062 тыс. руб. что говорит о положительной тенденции и может свидетельствовать об улучшении ситуации с оплатой продукции предприятии о выборе подходящей политики продаж. Рассматривая дебиторскую задолженность ООО «Белгородский завод «Энерготехмонтаж»»» следует отметить, что предприятие на 31.12.2017 г. имеет активное сальдо. В целом динамику изменения актива баланса можно назвать положительной

В части пассивов, увеличение валюты баланса в наибольшей степени произошло, в основном, за счет роста статьи «кредиторская задолженность» За прошедший период рост этой статьи составил 57 894 тыс. руб. (в процентном соотношении ее рост составил 61,99%.) Таким образом, на конец анализируемого периода значение статьи «Кредиторская задолженность» установилось на уровне 151 282 тыс. руб.

Рассматривая изменение собственного капитала ООО «Белгородский завод «Энерготехмонтаж»»» отметим, что его значение за анализируемый период значительно снизилось. На 31.12.2017 г. величина собственного капитала предприятия составила 1 345 тыс. руб. (0,22% от общей величины пассивов).

Доля заемных средств в совокупных источниках формирования активов за анализируемый период незначительно увеличилась. На 31.12.2017 г. совокупная величина заемных средств предприяти составила 600 917 тыс. руб. (99,78% от общей величины пассивов). Увеличение заемных средств предприятия ведет к увеличению степени его финансовых рисков и может отрицательно повлиять на его финансовую устойчивость.

В общей структуре пассивов величина собственного капитала, которая на 31.12.2015 г. составляла 4 203 тыс. руб., снизилась на 2 858 тыс. руб. (темп прироста составил -68%), и на 31.12.2017 г. его величина составила 1 345 тыс. руб. (0,22 % от общей структуры имущества). В наибольшей степени это изменение произошло за счет снижения статьи «нераспределенная прибыль (непокрытый убыток)» - на -2 858 тыс. руб.

На 31.12.2017 г. в общей структуре задолженности краткосрочные пассивы превышают долгосрочные на 477 471 тыс. руб. что при существующем размере собственного капитала и резервов может негативно сказаться на финансовой устойчивости предприятия.

Долгосрочная кредиторская задолженность, величина которой на 31.12.2015 г. составляла 44 538 тыс. руб., возросла на 17 185 тыс. руб. (темп прироста составил 38,59%), и на 31.12.2017 г. ее величина составила 61 723 тыс. руб. (10,25% от общей структуры имущества). Наибольшее влияние на увеличение долгосрочных пассивов оказал рост статьи «заемные средства».

Наибольший удельный вес в структуре краткосрочной кредиторской задолженности на 31.12.2017 г. составляет статья «заемные средства». На конец анализируемого периода величина задолженности по данной статье составляет 387 912 тыс. руб. (доля в общей величине краткосрочной дебиторской задолженности 71%). За анализируемый период снижение по этой статье задолженности составило 5,19%, что в абсолютном выражении составило -21 243 тыс. руб.

Таким образом, изменение за анализируемый период структуры пассивов следует признать в подавляющей части негативным.

Анализ ликвидности баланса по относительным показателям за весь рассматриваемый период представлен в таблице 2.6.

Таблица 2.6

Анализ ликвидности баланса по относительным показателям

Наименование	2015 г. тыс. руб.	2016 г. тыс. руб.	2017 г. тыс. руб.	Абсолютное отклонение (+;-)		Относительное отклонение (%)	
				2016/ 2015	2017/ 2016	2017/ 2015	2017/ 2016
Коэффициент абсолютной ликвидности	0,09	0,02	0,01	-0,07	-0,08	-77,7	-88,8
Коэффициент промежуточной (быстрой) ликвидности	0,75	0,60	0,61	-0,15	-0,14	-20,07	-18,43
Коэффициент текущей ликвидности	1,05	0,99	1,04	-0,06	-0,01	-5,71	-0,95
Коэффициент покрытия оборотных средств собственными источниками формирования	0,05	0,01	0,04	-0,06	-0,01	-114,31	-25,87
Коэффициент восстановления (утраты) платежеспособности	-	0,48	0,53	-	-	-	-

Коэффициент абсолютной ликвидности и на начало и на конец анализируемого периода (31.12.2015 г. - 31.12.2017 г.) находится ниже нормативного значения (0,2), что говорит о том, что значение коэффициента слишком низко и предприятие не в полной мере обеспечено средствами для своевременного погашения наиболее срочных обязательств за счет наиболее ликвидных активов. На начало анализируемого периода - на 31.12.2017 г. значение показателя абсолютной ликвидности составило 0,09. На конец анализируемого периода значение показателя снизилось, составив 0,01.

Коэффициент промежуточной (быстрой) ликвидности показывает, какая часть краткосрочной задолженности может быть погашена за счет наиболее ликвидных и быстро реализуемых активов. Нормативное значение показателя - 0,6-0,8, означающее, что текущие обязательства должны покрываться на 60-80% за счет быстрореализуемых активов. На начало анализируемого периода (на 31.12.2015 г.), значение показателя быстрой (промежуточной) ликвидности составило 0,75. На 31.12.2017 г. значение показателя снизилось, что можно рассматривать как отрицательную тенденцию, и составило 0,61.

Коэффициент текущей ликвидности и на начало и на конец анализируемого периода (31.12.2015 г. - 31.12.2017 г.) находится ниже нормативного значения 2, что говорит о том, что значение коэффициента достаточно низкое и предприятие не в полной мере обеспечено собственными средствами для ведения хозяйственной деятельности и своевременного погашения срочных обязательств.

Так как на конец анализируемого периода коэффициент текущей ликвидности находится ниже своего нормативного значения 2, и коэффициент текущей ликвидности ниже своего (0,1), рассчитывается показатель восстановления платежеспособности предприятия.

Показатель восстановления платежеспособности говорит о том, сможет ли предприятие, в случае потери платежеспособности в ближайшие шесть

месяцев ее восстановить при существующей динамике изменения показателя текущей ликвидности.

На конец периода значение показателя установилось на уровне 0, что говорит о том, что предприятие не сможет восстановить свою платежеспособность, так как показатель меньше единицы.

Далее проведем анализ финансовой устойчивости предприятия по абсолютным показателям (таблица 2.7).

Таблица 2.7

Анализ финансовой устойчивости предприятия по абсолютным показателям за 2015-2017 годы

Показатели	2015 г. тыс. руб.	2016 г. тыс. руб.	2017 г. тыс. руб.	Абсолютное отклонение (+;-)		Относительное отклонение (%)	
				2016/ 2015	2017/ 2016	2017/ 2015	2017/ 2016
1	2	3	4	5	6	7	8
1. Источники собственных средств	4 203	-16 403	1 345	-20 606	-2 858	-490,27	-68
2. вне оборотные активы	22 190	29 939	42 236	7 749	20 046	34,92	90,34
3. Источники собственных оборотных средств для формирования запасов и затрат	-17 987	-46 342	-40 891	-28 355	-22 904	-157,64	-127,34
4. Долгосрочные кредиты и займы	44 538	42 637	61 723	-1 901	17 185	-4,27	38,59
5. Источники собственных средств, скорректированные на величину долгосрочных заемных средств	26 551	-3 705	20 832	-30 256	-5 719	-113,95	-21,54
6. Краткосрочные кредитные и заемные средства	409 155	420 183	387 912	11 028	-21 243	2,70	-5,19
7. Общая величина	435 706	416 478	408 744	-19 228	-26 962	-4,41	-6,19

источников средств с учетом долгосрочных и краткосрочных заемных средств							
8. Величина запасов и затрат, обращающихся в активе баланса	145 251	193 768	206 334	48 517	61 083	33,40	42,05

Продолжение таблицы 2.7

1	2	3	4	5	6	7	8
9. Излишек источников собственных оборотных средств	-163 238	-240 110	-247 225	-76 872	-83 987	- 47,09	-51,45
10. Излишек источников собственных средств и долгосрочных заемных источников	-118 700	-197 473	-185 502	-78 773	-66 802	- 66,36	-56,28
11. Излишек общей величины всех источников для формирования запасов и затрат	290 455	222 710	202 410	-67 745	-88 045	- 23,32	-30,31

Проводя анализ типа финансовой устойчивости предприятия по абсолютным показателям, основываясь на трехкомплексном показателе финансовой устойчивости, в динамике заметна стагнация финансовой устойчивости предприятия.

Как видно из таблицы 2.10 и на 31.12.2015 , и на 31.12.2017 финансовую устойчивость ООО «Белгородский завод «Энерготехмонтаж»» по 3-х комплексному показателю можно охарактеризовать как «допустимо неустойчивое состояние предприятия», так как на начало анализируемого периода для финансирования запасов и затрат предприятие использует собственные, а также долгосрочные и краткосрочные заемные средства., а на конец периода для финансирования запасов и затрат предприятие использует собственные, а также долгосрочные и краткосрочные заемные средства.

Анализ показателей финансовой устойчивости за весь рассматриваемый период представлен в таблице 2.8.

Коэффициент автономии, за анализируемый период снизился на -0,01 и на 31.12.2017 г. составил 0,01. Это ниже нормативного значения (0,5) при котором заемный капитал может быть компенсирован собственностью предприятия.

Таблица 2.8

Анализ финансовой устойчивости по относительным показателям

Наименование	2015 г.	2016 г.	2017 г.	Абсолютное отклонение (+;-)		Относительное отклонение (%)	
				2016/ 2015	2017/ 2016	2017/ 2015	2017/ 2016
Коэффициент автономии	0,01	-0,03	0,01	-0,04	-	-200	-
Коэффициент отношения заемных и собственных средств (финансовый рычаг)	130,16	-34,27	446,78	-164,43	316,62	-73,67	243,2
Коэффициент соотношения мобильных и иммобилизованных средств.	23,84	17,23	13,26	-6,61	-10,58	-27,74	-44,39

Коэффициент маневренности	-0,37	-1,77	-0,65	-1,40	-0,28	-378,68	-75,69
Коэффициент обеспеченности запасов и затрат собственными средствами	0,18	-0,02	0,10	-0,20	-0,08	-110,46	-44,77
Коэффициент имущества производственного назначения	0,30	0,41	0,41	0,11	0,11	34,95	35,89
Коэффициент долгосрочно привлеченных заемных средств	0,91	1,63	0,98	0,71	0,06	77,86	7,10
Коэффициент краткосрочной задолженности	74,79	74,74	64,55	-0,05	-10,24	-0,06	-13,69
Коэффициент кредиторской задолженности	17,07	17,67	25,18	0,60	8,10	3,54	47,48

Коэффициент отношения заемных и собственных средств (финансовый рычаг), за анализируемый период увеличился на 316,61 и на 31.12.2017 г. составил 446,78. Чем больше этот коэффициент превышает 1, тем больше зависимость предприятия от заемных средств. Допустимый уровень часто определяется условиями работы каждого предприятия, в первую очередь, скоростью оборота оборотных средств. Поэтом дополнительно необходимо определить скорость оборота материальных оборотных средств и дебиторской задолженности за анализируемый период. Если дебиторская задолженность оборачивается быстрее оборотных средств, что означает довольно высокую интенсивность поступления на предприятие денежных средств, т.е. в итоге - увеличение собственных средств. Поэтому при высокой оборачиваемости материальных оборотных средств и еще более высокой оборачиваемости дебиторской задолженности коэффициент соотношения собственных и заемных средств может намного превышать 1.Коэффициен соотношения мобильных и иммобилизованных средств, за анализируемый период снизился на -10,58 и на 31.12.2017 г. составил 13,26. Коэффициент определяется как отношение мобильных средств (итог по второму разделу) и долгосрочной дебиторской задолженности к иммобилизованным средствам (вне оборотные активам, скорректированным на дебиторскую задолженность долгосрочного характера). Нормативное значение специфично для каждой отдельной отрасли, но при прочих равных условиях увеличение коэффициента является положительной тенденцией. Коэффициент маневренности за анализируемый период снизился на -0,28 и на 31.12.2017 г. составил -0,65. Это ниже нормативного значения (0,5). Коэффициент маневренности характеризует, какая дол источников собственных средств находится в мобильной форме. Нормативно значение показателя зависит от характера деятельности предприятия: в фондоемких производствах его нормальный уровень должен быть ниже, чем в материалоемких. На конец анализируемого периода ООО «Белгородский завод «Энерготехмонтаж»» обладает легкой структурой активов. Доля основных средств в валюте баланса менее 40 %. Таким образом, предприятие нельзя причислить к фондоемким производствам.

Коэффициент обеспеченности запасов и затрат собственными средствами, за анализируемый период снизился на -0,08 и на 31.12.2017 г. составил 0,1. Это ниже нормативного значения (0,6-0,8). Предприятие испытывает недостаток собственных средств для формирования запасов и затрат, что показал и анализ показателей финансовой устойчивости в абсолютном выражении. Коэффициент равен отношению разности между суммой источников собственных оборотных средств, долгосрочных кредитов и займов и вне оборотных активов к величине запасов и затрат.

Далее проведем анализ показателей рентабельности предприятия.

Значения показателей рентабельности ООО «Белгородский завод «Энерготехмонтаж»» за весь рассматриваемый период представлены в таблице 2.9.

Таблица 2.9

Показатели рентабельности

Наименование	2015 г.	2016 г.	2017 г.	Абсолютное отклонение (+;-)		Относительное отклонение (%)	
				2016/ 2015	2017/ 2016	2017/ 2015	2017/ 2016
Рентабельность продаж, %	1,44	2,80	2,08	1,35	0,64	93,72	44,24
Рентабельность собственного капитала, %	-601,95	-337,80	-235,73	939,75	1 241,75	156,12	206,29
Рентабельность оборотных активов, %	-4,78	-3,99	3,17	0,79	7,95	16,46	166,28
Общая рентабельность производственных фондов, %	-15,31	-7,44	8,13	7,86	23,43	51,38	153,09

Рассматривая показатели рентабельности, прежде всего следует отметить, что и на начало, и на конец анализируемого периода частное от деления прибыли до налогообложения и выручки от реализации (показатель общей рентабельности) находится у ООО «Белгородский завод «Энерготехмонтаж»» ниже среднеотраслевого значения, установившегося на уровне 10%.

За анализируемый период значения большинства показателей рентабельности увеличились, что следует скорее рассматривать как положительную тенденцию. Анализ показателей деловой активности (в днях) за весь рассматриваемый период представлен в таблице 2.10.

Таблица 2.10

Показатели деловой активности

Наименование	2015 г.	2016 г.	2017 г.	Абсолютное отклонение (+;-)		Относительное отклонение (%)	
				2016/ 2015	2017/ 2016	2017/ 2015	2017/ 2016
Оборачиваемость материальных запасов, об.	13,37	11,32	11,62	-2,04	-1,74	-15,28	-13,05
Оборачиваемость дебиторской задолженности, об.	5,87	6,05	6,24	0,17	0,37	2,97	6,29
Оборачиваемость прочих оборотных активов, об	313,66	237,42	139,05	-76,24	-174,61	-24,31	-55,67
Оборачиваемость кредиторской задолженности, об	20,76	19,90	16,69	-0,86	-4,07	-4,14	-19,60

Как видно из таблицы большинство показателей оборачиваемости за анализируемый период снизилось. Снижение периода оборачиваемости говорит о положительное тенденции. Также положительной тенденцией является то, что при снижении периода оборачиваемости увеличилась и выручка. За период с 31.12.2015 г. по 31.12.2017 г. выручка от реализации увеличилась на 5,32 %.

Далее оценим вероятность банкротства предприятия по наиболее часто используемым методикам, а именно по методике Альтмана, Таффелера и Лиса, результаты расчетов сведем в таблицу 2.11.

Оценив данные, представленные в таблице, можно сделать вывод, что в настоящее время вероятность банкротства предприятия можно оценить как низкую.

Таблица 2.11

Оценка вероятности банкротства предприятия

Наименование	31.12.2015 г.	31.12.2016 г.	31.12.2017 г.
5 - и факторная модель Альтмана (Z-счет)			
Значение коэффициента	3,75	3,79	3,67
Вероятность банкротства	вероятность банкротства ничтожна	вероятность банкротства ничтожна	вероятность банкротства ничтожна
4-х факторная модель Таффлера			
Значение коэффициента	0,82	0,83	0,85
Вероятность банкротства	вероятность банкротства мала	вероятность банкротства мала	вероятность банкротства мала
4-х факторная модель Лиса			
Значение коэффициента	0,06	0,07	0,07
Вероятность банкротства	положение предприятия устойчиво	положение предприятия устойчиво	положение предприятия устойчиво

Далее оценим основные производственные показатели экономической безопасности предприятия. В настоящее время выпуск важнейших видов продукции характеризуется данными:

- комплектные трансформаторные подстанции (КТП) - объем выпуска составляет около 70% от всей выпущенной продукции;
- комплектные двухтрансформаторные подстанции наружной установки (2КТП) - 12 % от всей выпущенной продукции;
- вакуумные выключатели - 10 % от всей выпущенной продукции;
- трансформаторы – 8 % от всей выпущенной продукции.

На рисунке 2.2 приведена структура основной производимой продукции предприятия.

Рис. 2.2. Структура основной производимой продукции предприятия

Динамика объема производства основных видов продукции предприятия представлена в таблице 2.12.

Таблица 2.12

Динамика объема производства основных видов продукции предприятия

Наименование продукции	2015 г.	2016 г.	2017 г.	Абсолютное отклонение, 2017 г./2015 г., тыс. руб.	Относительное отклонение, 2017 г./2015 г., %
Комплектные трансформаторные подстанции (КТП), шт.	7588	9019	9778	2190	28,8
Комплектные двухтрансформаторные подстанции наружной установки (2КТП) , шт.	528	547	552	24	4,5

Вакуумные выключатели, шт.	1256	1498	1659	403	32
Трансформаторы, шт.	184899	212573	240127	55228	29,8

Можно сделать вывод, что выпуск продукции предприятия растет, так выпуск комплектных трансформаторных подстанций за анализируемый период вырос на 28,8 %, выпуск комплектных двухтрансформаторных подстанций вырос на 4,5 %, выпуск вакуумных выключателей вырос на 32 %, выпуск трансформаторов вырос на 29,8 %.

Динамика объема продаж представлена на рисунке 2.3.

Рис. 2.3. Динамика объема продаж

Темп роста объема продаж составил 5,32 %. Наибольшим спросом пользуется такая продукция, как комплектные трансформаторные подстанции (КТП) и комплектные двухтрансформаторные подстанции наружной установки (2КТП).

Предприятие активно инвестирует средства на развитие производства. Динамика средств, направленных на развитие применяемых технологий на предприятии представлена в таблице 2.13.

Таблица 2.13

Динамика средств, направленных на развитие применяемых технологий на предприятии, тыс. руб.

Наименование	2015 г.	2016 г.	2017 г.	Абсолютное отклонение		Относительное отклонение	
				2016 г. к 2015 г.	2017 г. к 2015 г.	2016 г. к 2015 г.	2017 г. к 2015 г.
Технологии производства комплектных трансформаторных подстанций, тыс. руб.	2134	3455	4122	1321	1988	62	93
Технология производства комплектных двухтрансформаторных подстанции наружной установок, тыс. руб.	547	633	670	86	1217	16	22
Технологии производства вакуумных выключателей и трансформаторов, тыс. руб.	122	145	148	23	26	19	21

На рисунке 2.4 приведена динамика средств, направленных на развитие применяемых технологий на предприятии.

Рис. 2.4. Динамика средств, направленных на развитие применяет технологий на предприятии

Можно сделать вывод, что наибольшее количество средств тратиться на технологии производства комплектных трансформаторных подстанций, их количество возросло за 3 года на 93 %, наименьшее количество средств направляется в технологию производства вакуумных выключателей и трансформаторов, 148000 рублей за 2017 год, количество средств за 3 года возросло на 21 %.

Оценка конкурентной ситуации на рынке электротехнической продукции

Анализ конкурентной ситуации на рынке осуществляется в два этапа:

- определение главных конкурентных сил на рынке;

- анализ конкурентного положения основных компаний-производителей и формулирование альтернативных вариантов конкурентной стратегии ООО «Белгородский завод «Энерготехмонтаж»».

Размер рынка силовых трансформаторов оценивается в 46200 шт. в год, а скорость роста достигает 20% в год.

В таблице 2.14 приведена оценка привлекательности рынка электротехнической продукции. Каждому показателю приписывается вес, соответствующий его степени важности среди выбранных показателей.

Таблица 2. 14

Оценка привлекательности рынка электротехнической продукции

Показатели оценки	Значимость показателя	Привлекательность		
		Низкая	Средняя	Высокая
	Оценка	3	6	9
1. Емкость рынка	0,20	-	-	1,8
2. Темпы роста рынка	0,15	-	-	1,35
3. Сезонность	0,02	-	0,12	-
4. Конкуренция на рынке	0,08	-	-	0,72
5. Барьеры для вступления/выхода на рынок	0,15	-	-	1,35
6. Рентабельность продукции	0,05	-	0,3	-
7. Уровень технологии	0,10	-	0,6	-
8. Законодательство	0,05	-	-	0,45
9. Доступность персонала	0,15	-	0,9	-
10. Юридические и политические аспекты	0,05	0,15	-	-
Итого	1,00	0,15	1,92	5,67

Таким образом, рынок электротехнической продукции характеризуется высокой степенью привлекательности.

Доля рынка, уровень прибыли определяется тем, насколько эффективно ООО «Белгородский завод «Энерготехмонтаж»» противодействует главным источникам конкурентного давления, существующим на рынке, т.е.:

- внутриотраслевой конкуренцией и ее интенсивности;

- проникающим на рынок новым конкурентам.

Вновь появляющиеся компании приносят с собой новые производственные мощности и желание завоевать устойчивое положение на рынке. К их числу можно отнести АО «OREMI» – производитель в области электротехнической продукции.

- воздействию поставщиков.

Как правило, поставщики оказывают давление при заключении договоров, увеличивая цены или снижая качество предлагаемых сырья, материалов и комплектующих.

- воздействию покупателей.

В таблице 2.15 приведена оценка влияния конкурентных сил на эффективность деятельности ООО «Белгородский завод «Энерготехмонтаж»» и его основных конкурентов, т.е. определен характер конкуренции.

Таблица 2.15

Оценка влияния конкурентных сил на характер конкуренции

Конкурентные силы	Значимость показателя	Мощность конкурентной силы		
		Сильная	Умеренная	Слабая
	Оценка	9	6	3
1. Конкуренция на рынке и ее интенсивность	0,40	3,6	-	-
2. Опасность потенциального входа нового конкурента	0,30	-	-	0,9
3. Рыночная власть (воздействие) поставщиков сырья, материалов и комплектующих	0,10	-	0,6	-
4. Рыночная власть (воздействие) потребителей	0,20	-	1,2	-
Итого	1,00	3,6	1,8	0,9

Таким образом, на рынке жесткий характер конкуренции, причем наиболее влиятельной конкурентной силой является соперничество межд1 существующими компаниями-производителями электротехнического оборудования.

В этой ситуации удерживать завоеванные позиции ООО «Белгородский завод «Энерготехмонтаж»» помогают следующие его преимущества перед конкурентами:

– достаточно высокий объем выпуска силовых трансформаторов;

– достаточно большой опыт;

– наличие возможности разработки и выпуска трансформаторов с особыми параметрами (нестандартных);

– наличие современных технологических линий;

– адекватными финансовыми ресурсами;

– персонал ООО «Белгородский завод «Энерготехмонтаж»»» имеет достаточно высокий уровень профессионализма;

– соответствие системы менеджмента качества ООО «Белгородский завод «Энерготехмонтаж»»» международным стандартам;

– широкая известность и признание на российском рынке;

– относительно высокое качество.

Наряду с этим некоторые недостатки как технологического, так и организационного характера негативно сказываются на конкурентоспособности завода. К ним относятся:

– ограниченные возможности выпуска трансформаторов мощностью от 630 кВА и выше;

– физический износ оборудования достигает 80%;

– отсутствие комплексного подхода к технологическому развитию производства;

– отсутствие реальных решений по автоматизации производственных процессов;

– разработана и внедряется заведомо низкоэффективная программа по снижению затрат;

– отсутствие четкого стратегического направления, а также несвоевременное принятие решений, бюрократия;

– отсутствие маркетингового образа мышления в большинстве структурных подразделений;

– отношение к потребителю как к партнеру неудовлетворительное;

– эффективность сформированной сети официальных представителей снижается;

– сроки исполнения заказа (т.е. период времени от подачи заявки до момента отгрузки) не удовлетворяют потребителя.

Исходя из обозначенных выше конкурентных преимуществ и недостатков в таблице 2.16 оценена конкурентная позиция ООО «Белгородски завод «Энерготехмонтаж»».

Таблица 2.16

Оценка конкурентной позиции

ООО «Белгородский завод «Энерготехмонтаж»»

Показатели оценки	Значимость показателя	Конкурентная позиция		
		Низкая	Средняя	Высокая
	Оценка	3	6	9
1. Занимаемая доля рынка	0,25	-	-	2,25
2. Наличие собственной торговой сети	0,15	-	0,9	-
3. Имидж ООО «Белгородский завод «Энерготехмонтаж»»	0,10	-	-	0,9
4. Развитость службы маркетинга	0,10	-	0,6	-
5. Состояние производства (развитость процессов)	0,10	0,3	-	-
6. Уровень менеджмента (управления)	0,05	0,15	-	-
7. Качество обслуживания	0,03	-	0,18	-
8. Финансовые возможности	0,07	-	0,42	-
9. Привлекательность продукции	0,05	-	-	0,45
10. Уровень цен	0,10	0,3	-	-
Итого	1,00	0,75	2,10	3,60

Занимаемая ООО «Белгородский завод «Энерготехмонтаж»» конкурентная позиция оценивается как высокая.

Основными направлениями стратегического развития предприятия в 2018 году являются:

– расширение ассортимента производимой продукции;

– техническое перевооружение и реконструкция предприятия с целью обновления основных фондов, внедрение высокоэффективных энергосберегающих технологий;

– применение новых технологий производства

– укрепление экспортного потенциала;

– подготовка и повышение квалификации производственных и научных кадров.

Далее проанализируем социальные показатели экономической безопасности предприятия. На первом этапе анализа проанализируем движение кадров на предприятии (таблица 2.17).

Таблица 2.17

Анализ движения кадров на предприятии ООО «Белгородский «Энерготехмонтаж»» за 2015–2017 гг.

Показатели	Год			Абсолютное отклонение (+,-)		Относительное отклонение (%)	
	2015	2016	2017	2016/2015	2017/2015	2016/2015	2017/2015
Удельный вес рабочих в ППП, %	83,4	82,4	86,7	-1	3,3	-1,1	3,9
Число отработанных человеко-часов	295342	359670	423998	64328	128656	21,7	43,5
Среднечасовая выработка на 1 рабочего, тыс. руб./чел.	1,56	2,58	2,95	1,02	1,39	65,3	89,1
Число принятых, чел.	18	1	5	-17	-13	-94,4	-72,2
Число уволенных, чел.	13	14	2	1	-11	7,6	-84,6
Коэффициент оборота по	0,0	0,	0,0	-0,017	-0,013	-94,4	-72,2

приему	18	001	05				
Коэффициент оборота по увольнению	0,013	0,013	0,002	-	0,011	-	-84,6

Анализ показал, что число принятых работников сократилось на 72,2 %, уволенных на 84,6 %. Среднечасовая выработка работников увеличилась на 89,1 %, что положительно характеризует деятельность предприятия.

Рассмотрим виды обучения персонала и проанализируем структуру профессионального обучения рабочих по видам в таблице 2.18.

Таблица 2.18

Анализ структуры профессионального обучения работников ООО «Белгородский завод «Энерготехмонтаж»» по видам обучения

Наименование показателя	2015 г.		2016 г.		2017 г.	
	чел.	%	чел.	%	чел.	%
Численность работников, прошедших обучение за год, чел.	88	100	250	100	184	100
в т. ч.:						
повысили квалификацию	73	82,8	234	93,6	164	89,1
прошли стажировку	3	3,3	2	0,9	2	1,2
прошли профессиональную подготовку и переподготовку	12	13,9	14	5,5	18	9,7

Анализ структуры подготовки сотрудников показывает, что основным типом обучения было повышение квалификации. Например в 2017 году повысили свою квалификацию 89,1%, прошли обучение на 1,2%. Доля прошедших профессиональную подготовку и переподготовку - 9,7%. В течение анализируемого периода в структуре профессиональной подготовки изменилось, но произошедшие изменения не могут быть значительными. В 2017 году темпы подготовки персонала снизился по сравнению с 2016 годом и составил 154,3%, а в 2016 году составил 201,3%. Этот процесс показан в таблице. Анализируя динамику категорий, мы можем сказать, что устойчивый рост числа обученных работников наблюдалась только среди руководителей.

В 2017 году он увеличился на 52% по сравнению с началом анализируемого периода. В 2016 году произошло резкое увеличение числа подготовленных специалистов и рабочих. В этом году расходы на образование увеличилась в 2,4 раза. В 2016 году компания снизила темп обучения, но на снижение затрат на одного сотрудника данный процесс не повлиял.

Положительной тенденцией является снижение средней частоты обучения руководителей. Это говорит о том, что компания увеличила частоту подготовки работников этой категории. Тенденция в средней частоты подготовки специалистов нельзя назвать устойчивым. Об этом свидетельствует тот факт, что в 2015 году средняя их частота значительно снизилась, но в следующем году она снова увеличилась. Таким образом, менеджеры компании проходят обучение в один раз в 2 года, и специалисты - один раз в 4 года.

Таблица 2.19

Динамика профессионального обучения

в ООО «Белгородский завод «Энерготехмонтаж»»

Наименование показателя	2015 г.	2016 г.	2017 г.
1. Темп изменения численности обученных, %			
1.1 Всего персонала	100,0	201,3	154,3
1.2 Руководителей	100,0	138,0	152,0
1.3 Специалистов	100,0	188,8	136,0
1.4 Рабочих	100,0	208,3	156,3

2. Средняя периодичность обучения руководителей, лет	2,8	2,0	1,9
3. Средняя периодичность специалистов, лет	5,3	2,8	3,9
4. Собственные затраты предприятия на обучение, тыс. руб.	172 155,0	41 6236,0	594 900,0
4.1 На одного работника, тыс. руб./чел.	26,9	63,6	88,4
5. Темп изменения собственных затрат на обучение, раз	1,0	2,4	1,4

На основе этого анализа мы можем сказать, что:

- за анализируемый период увеличился уровень квалификации всего персонала, что подтверждается увеличением среднего тарифа разряда персонала на 7,7%, в том числе средний уровень специалистов -на 4,6%, рабочих - на 11,6%;

- в целом мы можем говорить о повышении профессионального уровня персонала, его совершенствования и развития. В 2017 году, количество обученных за год составила 184 человек и превысило число обученных в 2015 среди категорий наибольшую долю обученных на протяжении анализируемого периода составляли рабочие – более 80%;

- к концу периода увеличилась частота обучения руководителей, о чем говорит снижение коэффициента периодичности. Периодичность обучения специалистов, наоборот, увеличилась. Это значит, что обучаться они стали реже.

На основе собранной и проанализированной информации можно сделать вывод, что компания имеет высокий уровень трудового потенциала. Об этом свидетельствует прежде всего, увеличение численности промышленно-производственного персонала. Во-вторых, высокий уровень образования работников, и его рост, рост квалификации персонала, увеличение частоты обучение руководителей и специалистов в рассматриваемый период.

В-третьих, активизация усилий предприятия по развитию персонала, что привело к увеличению количества подготовленных к концу 2017 года, и увеличение собственных затрат предприятия на одного работника. В итоге можно сказать, что в конце 2017 года, компания имеет высокий уровень трудового потенциала для удовлетворения потребностей производства. Основная задача предприятия в сфере формирования кадровой политики является создании команды, состоящей из высококвалифицированных работников, которые стремятся реализовать свой потенциал в решении технических, экономических и социальных задач.

Создание условий для оптимального использования кадрового потенциала, укрепление единой корпоративной культуры, эффективной системы мотивации и профессионального развития сотрудников.

Целью кадровой политики ООО «Белгородский завод «Энерготехмонтаж»» является формулирование основных принципов управления персоналом и характеристике основных направлений системы управления персоналом.
Основной принцип кадровой политики организации является ее направленность на обеспечение баланса между экономической и социальной эффективности человеческих ресурсов. Экономическая эффективность использования результатов профессиональной деятельности сотрудников ООО для достижения стратегических целей и задач предприятия.

Социальная эффективность-создание условий для удовлетворения социально-экономических ожиданий, потребностей и интересов работников предприятия. Ключевые принципы деятельности кадровой политики приведены в таблице 2.16.

Таблица 2.20

Ключевые принципы деятельности кадровой политики

ООО «Белгородский завод «Энерготехмонтаж»»

Принципы	Описание

Доступность и открытость для персонала ООО «Белгородский завод «Энерготехмонтаж»»	На предприятии работники оповещаются о всех нововведениях в области кадрового управления.
Гибкость	Возможность применения в условиях динамичных организационных, экономических, а также внешних изменений.
Обязательность	Для исполнения работниками любого должностного уровня принципов политики по управлению персоналом.
Универсальность	Направленность на обеспечение комплекса мер, позволяющих решить любые производственные, профессиональные и социальные ситуации.
Совершенствование	Постоянное совершенствование методов управления персоналом на основе современных концепций управления персоналом с учетом особенностей и стандартов ООО «Белгородский завод «Энерготехмонтаж»».
Эффективность	Соответствие затрат полученным результатам по количеству и качеству.
Объективность	Обеспечение непредвзятого, всестороннего подхода.
Преемственность	Обозначение долгосрочных ключевых принципов политики в области управления персоналом ООО «Белгородский завод «Энерготехмонтаж»».

Проанализируем основные направления кадровой политики ООО «Белгородскийзавод «Энерготехмонтаж»»:

1. Положение компании в области людских ресурсов, планирование персонала, поиск персонала. подбор персонала.

2. Использование персонала (адаптация персонала, мотивация персонала, оценка персонала, составление индивидуальных программ карьерного роста).

3. Управление знаниями в компании (централизации и систематизации знаний, коллективизация знаний, интенсивности создания и использования знания организация системы профессиональной подготовки персонала, организации.

4. Корпоративная культура (создание и продвижение).

1. Планирование потребности в персонале должно быть направлено на решение специфических задач управления персоналом. К числу таких задач относятся:

- точное определение организации (предприятия) для работников в плановом периоде;

- определение потребности в привлечении (или высвобождении) сотрудников в зависимости от перспектив развития предприятия в плановом периоде;

- обеспечение рационального использования кадрового потенциала организации (предприятия);

- разработка мер по развитию и обучению персонала в период планирования;

- определение затрат на персонал.

В ООО «Белгородский завод «Энерготехмонтаж»» развиты только некоторые элементы системы планирования потребности в персонале:

- меры по развитию и обучению персонала, на основе заявленных потребностей в обучении и развитии сотрудников и их руководителей готовиться учебный план работы на год, на основе этого плана, разрабатываются программы внутреннего обучения;

- сводный план обучения в компании, утверждает генеральный директор, прогнозируется сумма расходов на образование в годовом бюджете;

- определение фонда оплаты труда за год, с учетом запланированного повышения уровня оплаты труда, возможной реструктуризации изменений и др. в соответствии с планом развития организации за год;

- определение   расходов бюджета на подбор персонала;

- определение денежного фонда для дополнительных социальных выплат.

Остальные элементы системы планирования потребности в персонале развиты слабо и носят не системный характер.

Поиском, набором и отбором персонала в ООО «Белгородский завод «Энерготехмонтаж»» занимаются специалисты отдела службы по управлению и развитию персонала на основании поданной руководителем заявки на подбор персонала.

На этапе подбора персонала соискатели заполняют анкеты и листы самоанализа, проходят собеседование с менеджером по персоналу он использует различные методы проведения интервью с кандидатом:

1) биографическое интервью;
2) case-интервью;
3) стресс-интервью;
4) интервью «20 граней».

На этапе отбора кандидаты проходят психологическую оценку. В 2017 году в ООО «Белгородский завод «Энерготехмонтаж»» психологическую оценку прошли 24 кандидата.

Большим недостатком кадровой политики является отсутствие кадрового резерва. Внедрение технологии кадрового резерва позволит оперативно закрывать вакансии, сократить затраты на подбор персонала, повысит мотивацию сотрудников, даст возможность карьерного роста опытным сотрудникам.

Большое число сотрудников увольняется в первый месяц работы на новом месте, чтоб избежать этого, в компании разработана и внедряется система адаптации и наставничества новых сотрудников. Положение о системе индивидуального наставничества апробировалось в июле 2016г. и вступило в действие с сентября 2016г. Система адаптации в ООО «Белгородский завод «Энерготехмонтаж»» включает в себя следующие составляющие:

1. Каждый вновь принятый в компанию сотрудник получает «Справочник новичка» он разработан и введен в использование для наиболее эффективного и оперативного ознакомления вновь принятых сотрудников с информацией о структуре компании, её истории, направлениях бизнеса, руководителях, корпоративном кодексе и корпоративных стандартах, а также образцами необходимых документов и списком «нужных» телефонов.

2. В первые две недели работы все новые сотрудники посещают

обучающее мероприятие, где получают более подробную информацию о структуре компании, направлениях ее деятельности, системе обучения и развития сотрудников компании, знакомятся с корпоративной культурой.

Так же этими документами руководствуются менеджеры по персоналу при подборе сотрудников на открытые вакансии.

Система мотивации персонала ООО «Белгородский завод «Энерготехмонтаж»» представляет собой совокупность систем материального и нематериального стимулирования сотрудников. Система мотивации персонала состоит из следующих компонентов:

– система прямой материальной мотивации;
– система косвенной материальной мотивации;
– система нематериальной мотивации.

Система прямой материальной мотивации персонала состоит из базового оклада и премиальных (переменная часть заработной платы и премия из фонда руководителя).

Таким образом, прямой материальной мотивацией в ООО «Белгородский завод «Энерготехмонтаж»» является заработная плата, которая зависит от занимаемой должности, квалификации, стажа работы, количества и качества затрачиваемого труда.

Система косвенной материальной мотивации - это так называемый компенсационный пакет (соцпакет), предоставляемый работнику. Компенсационный пакет - это бенефиты, предоставляемые сотруднику организации в зависимости от уровня его должности, профессионализма, авторитета.

Систем косвенного материального стимулирования анализируемого предприятия можно разделить на два блока:

1) обязательные бенефиты - регламентируются трудовым законодательством (оплата больничных листов, оплата ежегодных отпусков, обязательное медицинское страхование, отчисления на

обязательное пенсионное страхование);

2) добровольные бенефиты - используются работодателем на добровольной основе в соответствии с положением о социальных выплатах и льготах работникам, размер выплат корректируется ежегодно (бракосочетание, рождение ребенка, сильное повреждение или утеря имущества, смерть родственника 1-го круга).

3) система нематериальной мотивации - это совокупность внешних стимулов немонетарного характера, которые используются в организации для эффективного труда сотрудников. Практический опыт показывает, что зарплата и используемая система бенефитов (соцпакет) всегда являются решающим фактором повышения заинтересованности сотрудников к работе в тои или иной организации. Очень важным условием для решения данной задачи является использование методов нематериального стимулирования. В ООО «Белгородский завод «Энерготехмонтаж»» используются традиционные методы нематериального стимулирования, такие как:

– движение «вверх» по карьерной лестнице с повышением занимаемого статуса;

– приоритет при планировании отпуска;

– устная и/или письменная благодарность за эффективную работу по итогам работы за полгода и год, ценные призы (за полгода благодарность вручается при общем собрании коллектива структурной единицы генеральным директором, за год - на Новогоднем корпоративном мероприятии, так же вручаются ценные призы. Само Новогоднее мероприятие так же является методом нематериального стимулирования, т.к. проводится с приглашением артистов и полностью за счет компании);

– организация и проведение корпоративных мероприятий для сотрудников и их детей.

– в компании регулярно проводятся мероприятия по опытом.

Таким образом сделаем обобщающий вывод, характеризующий показатели экономической безопасности предприятия.

Оценка финансовой составляющей экономической безопасности предприятия показала, что выручка от реализации компании по сравнению с базовым периодом увеличилась (с 1 938 391 тыс. руб. на 31.12.2015 г. до 2 041 464 тыс. руб. на 31.12.2017 г.). За анализируемый период изменение объема продаж составило 103 073 тыс. руб. Темп прироста составил 5,32%. Валовая прибыль на 31.12.2015 г. составляла 374 790 тыс. руб. За анализируемый период она возросла на 111 тыс. руб., что следует рассматривать как положительный момент и на 31.12.2017 г. составила 374 901 тыс. руб. Прибыль от продаж на 31.12.2015 г. составляла 27 982 тыс. руб. За анализируемый период она, также как и валовая прибыль, возросла на 14 526 тыс. руб., и на 31.12.2017 г. прибыль от продаж составила 42 508 тыс. руб., также как и валовая прибыль, осталась на прежнем уровне.

Следует отметить высокий уровень коммерческих и управленческих расходов в структуре отчета о прибылях и убытках организации. На начало анализируемого периода их доля составляла 22,18 %, от себестоимости реализованной продукции, а на конец периода – 19,94 % от себестоимости проданных товаров, продукции, работ, услуг.

Показателем снижения эффективности деятельности предприятия можно назвать более высокий рост себестоимости по отношению к росту выручки. Рост себестоимости, в то время как выручка выросла на (5,32 %) составил 6,58 %). Отрицательным моментом является наличие убытков по прочим доходам и расходам. На 31.12.2017 г. сальдо по ним установилось на уровне -22 514 тыс. руб., однако наблюдается положительная тенденция – за период с конца 31.12.2015 г. по конец 31.12.2017 г. сальдо по прочим доходам и расходам увеличилось на 38 433 тыс. руб.

Чистая прибыль за анализируемый период выросла на 43 04 тыс. руб., и на конец 31.12.2017 г. установилась на уровне 17 748 тыс. руб. (темп прироста составил -170,15%). Размер дебиторской задолженности за анализируемый период в сумме снизился на 6 062 тыс. руб. что говорит о положительной тенденции и может свидетельствовать об улучшении ситуации с оплатой продукции предприятия и о выборе подходящей политики продаж. За анализируемый период значения большинства показателей увеличились, что следует скорее рассматривать как положительную тенденцию.

В настоящее время вероятность банкротства предприятия можно оценить как низкую.

Оценка производственной составляющей экономической безопасности предприятия показала, выпуск продукции предприятия растет, так выпуск комплектных трансформаторных подстанций за анализируемый период вырос на 28,8 %, выпуск комплектных двухтрансформаторных подстанций вырос на 4,5 %, выпуск вакуумных выключателей вырос на 32 %, выпуск трансформаторов вырос на 29,8 %.

Темп роста объема продаж составил 5,32 %. Наибольшим спросом пользуется такая продукция, как комплектные трансформаторные подстанции (КТП) и комплектные двухтрансформаторные подстанции наружной установки (2КТП).

Удерживать завоеванные позиции ООО «Белгородский завод «Энерготехмонтаж»» помогают следующие его преимущества перед конкурентами:

– достаточно высокий объем выпуска силовых трансформаторов;

– достаточно большой технологический опыт;

– наличие возможности разработки и выпуска трансформаторов с особыми параметрами (нестандартных);

– наличие современных технологических линий;

– адекватными финансовыми ресурсами;

– персонал ООО «Белгородский завод «Энерготехмонтаж»» имеет достаточно высокий уровень профессионализма;

– соответствие системы менеджмента качества ООО «Белгородский завод «Энерготехмонтаж»» международным стандартам;

– широкая известность и признание на российском рынке;

– относительно высокое качество.

Наряду с этим некоторые недостатки как технологического, так и организационного характера негативно сказываются на конкурентоспособности завода. К ним относятся:

– ограниченные возможности выпуска трансформаторов мощностью от 630 кВА и выше;

– физический износ оборудования достигает 80%;

– отсутствие комплексного подхода к технологическому развитию производства;

– отсутствие реальных решений по автоматизации производственных процессов;

– разработана и внедряется заведомо низкоэффективная программа по снижению затрат;

– отсутствие четкого стратегического направления, а также несвоевременное принятие решений, бюрократия;

– отсутствие маркетингового образа мышления в большинстве структурных подразделений;

– отношение к потребителю как к партнеру неудовлетворительное;

– эффективность сформированной сети официальных представителей снижается; – сроки исполнения заказа (т.е. период времени от подачи заявки до момента отгрузки) не удовлетворяют потребителя.

Оценка социальной составляющей экономической безопасности предприятия показала, что число принятых работников сократилось на 72,2 %, уволенных на 84,6 %. Среднечасовая выработка работников увеличилась на 89,1 %, что положительно характеризует деятельность предприятия.

Анализ структуры подготовки сотрудников показывает, что основным обучения было повышение квалификации. Например, в 2017 году повысили свою квалификацию 89,1%, прошли обучение на 1,2%. Доля прошедших профессиональную подготовку и переподготовку - 9,7%. В течение анализируемого периода в структуре профессиональной подготовки изменилось, но произошедшие изменения не могут быть значительными. В 2017 году темпы персонала снизился по сравнению с 2016 годом и составил 154,3%, а в 2016 году составил 201,3%. Этот процесс показан в таблице. Анализируя динамику категорий, мы можем сказать, что устойчивый рост числа обученных работников наблюдалась только среди руководителей.

В 2017 году он увеличился на 52% по сравнению с началом анализируемого периода. В 2016 году произошло резкое увеличение числа подготовленных и рабочих. В этом году расходы на образование увеличилась в 2,4 раза. В 2016 году компания снизила темп обучения, но на снижение затрат на одного сотрудника данный процесс не повлиял.

Положительной тенденцией является снижение средней частоты обучения руководителей. Это говорит о том, что компания увеличила частоту подготовки этой категории. Тенденция в средне частоты подготовки специалистов нельзя назвать устойчивым. Об этом свидетельствует тот факт, что в 2015 году средняя их частота значительно снизилась, но в следующем году она снова увеличилась. Таким образом, менеджеры компании проходят обучение в среднем один раз в 2 года, и специалисты - один раз в 4 года.

За анализируемый период увеличился уровень квалификации персонала, что подтверждается увеличением среднего тарифа разряда персонала на 7,7%, в том числе средний уровень специалистов -на 4,6%, рабочих - на 11,6%. В целом мы можем говорить о повышении профессионального уровня персонала, его совершенствования и развития. В 2017 году, количество обученных за год составила 184 человек и превысило число обученных в 2015 среди категорий наибольшую долю обученных на протяжении анализируемого периода составляли рабочие – более 80%.

Таким образом практически все индикаторы экономической безопасности находятся в пределах пороговых значений, а степень использования имеющегося потенциала близка установленным нормам и стандартам.

2.3. Анализ системы защиты информации на предприятии

Анализируя систему защиты информации на предприятии, можно сделать вывод, что конкретная служба по защите информации в ООО «Белгородский завод «Энерготехмонтаж»» отсутствует. Поэтому ответственность за защищаемую информацию несет специалист по управлению персоналом. Данная документация обрабатываются путем строгого контроля изъятия и возвращения документов под расписку уполномоченного работника. За информацию, относящуюся к коммерческой тайне, несут ответственность следующие служащие предприятия: начальники, бухгалтера, экономисты инженеры. Безопасность информации ООО «Белгородский завод «Энерготехмонтаж»» - 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 в ООО «Белгородский завод «Энерготехмонтаж»»:

- 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.

Для достижения целей защиты должно обеспечиваться эффективное решение следующих задач:

- защита от вмешательства в процесс функционирования предприятия посторонних лиц;

- защита от несанкционированных действий с информационными ресурсами предприятия посторонних лиц и сотрудников, не имеющих соответствующих полномочий;

- обеспечение полноты, достоверности и оперативности информационной поддержки принятия управленческих решений руководством предприятия;

- обеспечение физической сохранности технических средств и программного обеспечения предприятия и защита их от действия техногенных и стихийных источников угроз;

- регистрация событий, влияющих на безопасность информации, обеспечения полной подконтрольности и подотчетности выполнения всех операций, совершаемых на предприятии;

- своевременное выявление, оценка и прогнозирование источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба интересам субъектов, нарушению нормального функционирования и развития предприятия;

- анализ рисков реализации угроз безопасности информации и оценка возможного ущерба;

- обеспечение возможности восстановления актуального состояния предприятия при нарушении безопасности информации и ликвидации последствий этих нарушений;

- создание и формирование целенаправленной политики безопасности информации предприятия.

Информационная система ООО «Белгородский завод «Энерготехмонтаж»» охватывает все сферы его деятельности: административную, производственную, финансовую, выступает как связующее звено при выработке стратегии бизнеса и качества управления предприятием и персоналом. В ней содержатся сведения, касающиеся планов, состояния материальных и финансовых потоков, договорной деятельности, данные финансового и управленческого учета. Такого рода коммерческая информация носит сугубо конфиденциальный характер, а ее утрата может критичной для работы всего предприятия, поэтому организация работы пользователей с содержащейся в системе информацией требует специальных мер защиты, обеспечивающих конфиденциальность, целостность и доступность данных.

Исследуемое предприятие содержит следующие конкретные информационные ресурсы:

- информация, относящаяся к коммерческой тайне:

- заработная плата;

- договоры с поставщиками и покупателями;

- технологии производства;

- защищаемая информация:

- личные дела работников,

- трудовые договора,

- личные карты работников,

- содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности,

- прочие разработки и документы для внутреннего пользования;

- открытая информация:

- буклеты,

- информация на web-сайте

- учредительный документ, устав, прайс-лист продукции.

Угрозы информационной безопасности характерные для предприятия представлены в таблице 2.21.

Таблица 2.21

Угрозы и уязвимости на предприятии

Угроза	Уязвимости
Рабочее место сотрудника	
1. Физический доступ нарушителя к рабочему месту	1.Отсутствие системы контроля доступа сотрудников к чужим рабочим местам. 2. Отсутствие системы видеонаблюдения на предприятии
2. Разглашение конфиденциальной информации, хранящейся на рабочем месте сотрудника организации	1.Отсутствие соглашения о неразглашении между работником и работодателем. 2. Нечеткая регламентация ответственности сотрудников предприятия
3. Разрушение (повреждение, утрата) конфиденциальной информации при помощи специализированных программ и вирусов	1. Отсутствие ограничения доступа пользователей к сети интернет и к внутренней корпоративной сети
Конфиденциальная информация	
1.Физический доступ нарушителя к носителям	1.Неорганизованность контрольно-пропускного режима в организации 2.Отсутствие видеонаблюдения в организации
2. Разглашение конфиденциальной информации, используемой 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

На предприятии существует угрозы доступности, угрозы целостности и угрозы конфиденциальности информации.

1.Угрозами доступности информации являются: разрушение (уничтожение) информации: вирус, повреждение оборудования, чрезвычайная ситуация (пожар); отказ поддерживающей инфраструктуры: нарушение работы систем связи, электроэнергии, теплоснабжения, кондиционирования, повреждение помещения.

Мерами предотвращения данных угрозы может являться следующее:

1. Установка программы антивируса.

2. Осуществление резервного копирования данных на съемные носители для быстрого восстановления утерянных данных во время системной ошибки.

3. Установка аварийных источников бесперебойного питания.

4. Подвод электроэнергии не менее от двух независимых линий электропередачи.

5. Плановое обслуживание зданий и в целом всей поддерживающей инфраструктуры.

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

Мерами предотвращения данной угрозы может являться следующее:

1. Введение и частая смена паролей.

2. Использование криптографических средств защиты информации.

3. Угрозами конфиденциальности являются: кражи оборудования; делегирование лишних или неиспользуемых полномочий на носитель с конфиденциальной информацией; открытие портов; установка нелицензионного ПО; злоупотребления полномочиями.

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

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

Основными законодательными актами, регулирующими вопросы информационной безопасности предприятия, являются:

1. Гражданский кодекс РФ ст.139;

2. Уголовный кодекс гл.28 ст.272, 273, 274, 138, 183;

3. Закон Российской Федерации «Об информации, информатизации и защите информации»;

4. Закон Российской Федерации «О коммерческой тайне».

2. Административный уровень информационной безопасности.

Политика информационной безопасности пока не утверждена.

3. Организационный и программно-технический уровень уровень защиты информации.

Организационные меры являются решающим звеном формирования и реализации комплексной защите информации. Эти меры играют существенную роль в создании надежного механизма защиты информации, т.к. возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями, пользователей или персонала защиты. Программно-технические меры защиты информации - это совокупность аппаратных и программных средств и мероприятий по их использованию в интересах защиты конфиденциальности информации.

ООО «Белгородский завод «Энерготехмонтаж»» применяет следующие организационные и программно-технические меры для обеспечения безопасности информации (таблица 2.22).

Таблица 2.22

Организационные и программно-технические меры обеспечения информационной безопасности предприятия

Наименование	% использования
Защита от вредоносного ПО,%	60
Регулярное установление обновлений,5	20
Ограничение доступа к информации, %	10

Обеспечение физической безопасности IT систем,%	5
Шифрование деловой переписки, %	2
Специальная полтика безопасности для ноутбуков, используемых на предприятии, %	3

На рисунке 2.5 наглядно представлены основные меры применяемые ООО «Белгородский завод «Энерготехмонтаж»»» для обеспечения информационной безопасности

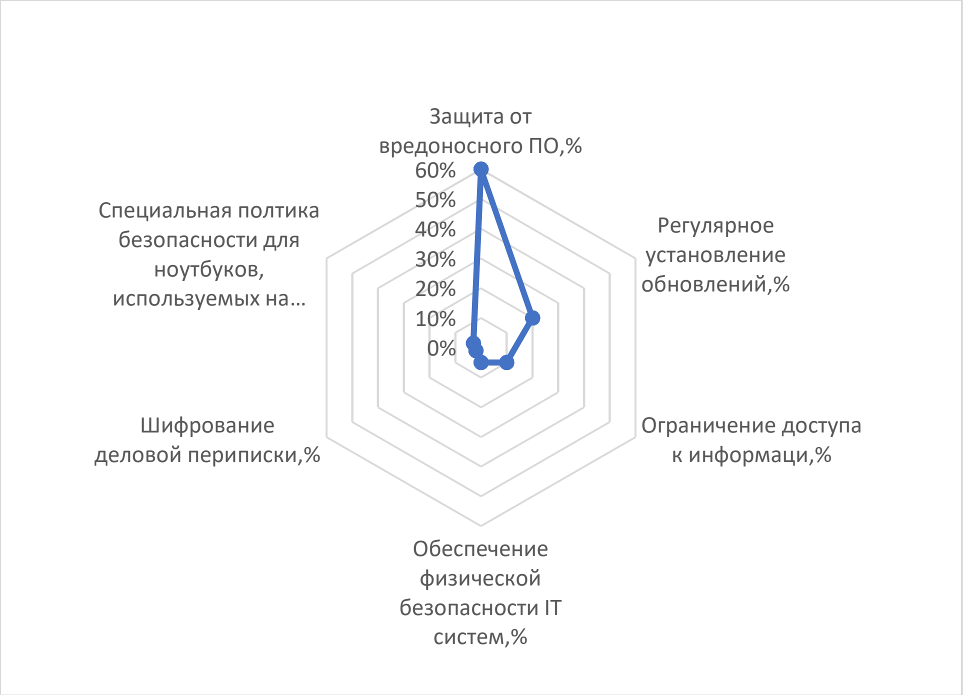


Рис. 2.5. Меры, применяемые ООО «Белгородский завод «Энерготехмонтаж»»» для обеспечения информационной безопасности

Проанализировав информационную безопасность предприятия можно сделать вывод, что информационной безопасности уделяется недостаточное внимание:

- отсутствует наличие программных средств для мониторинга информационной безопасности предприятия;

- отсутствует дополнительная защита файлов и информации (отсутствует элементарный запрос пароля при открытии изменении информации в файлах, не говоря уже о средствах шифрования данных);

- нерегулярное обновление баз программы антивируса и сканирование рабочих станций;

- большое количество документов на бумажных носителях в основном лежат в папках (иногда и без них) на рабочем столе сотрудника, что позволяет злоумышленникам без труда воспользоваться данного рода информациях в своих целях;

- не производится регулярное обсуждение вопросов информационной безопасности на предприятии и возникающих проблем в этой области;

- не организована регулярная проверка работоспособности информационных систем предприятия отладка производится только лишь в том случае, когда они выходят из строя;

- отсутствие политики информационной безопасности.

Все вышеперечисленное является очень важными недостатками обеспечения информационной безопасности предприятия.

ГЛАВА 3. РАЗРАБОТКА СИСТЕМЫ МЕР ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ ООО «БЕЛГОРОДСКИЙ ЗАВОД ЭНЕРГОТЕХМОНТАЖ»

3.1. Основные направления по совершенствованию защиты информации

В «Доктрине информационной безопасности Российской Федерации» защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере. К настоящему времени сложилась общепринятая точка зрения на концептуальные основы информационной безопасности. Суть ее заключается в том, что подход к обеспечению информационной безопасности должен быть комплексным, сочетающим меры следующих уровней:

- законодательного – федеральные и региональные законы, подзаконные и нормативные акты, международные, отраслевые и корпоративные стандарты;
- административного – действия общего и специального характера, предпринимаемые руководством организации;
- процедурного – меры безопасности, закрепленные в соответствующих методологиях и реализуемые ответственными менеджерами и персоналом предприятия;
- научно-технического – конкретные методики, программно-аппаратные, технологические и технические меры.

Главными принципами обеспечения безопасности в соответствии с законом РФ «О безопасности» являются:

- законность,
- соблюдение баланса жизненно важных интересов личности, общества и государства,

- взаимная ответственность перечисленных субъектов,
- интеграция системы безопасности в рамках компании, общества, государства,
- взаимодействие с международными системами безопасности.

Экономическую безопасность предпринимательской деятельности можно определить как «защищенность жизненно важных интересов государственного или 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.

Стратегия обеспечения экономической безопасности Российской Федерации строится на основании официально действующих правовых и нормативных актов, основными из которых являются: Конституция Российской Федерации; Закон «О безопасности» от 5 марта 1992 г. с изменениями и дополнениями от 25 декабря 1992 г.; Государственная стратегия экономической безопасности РФ (Основные положения), одобренная Указом Президента РФ № 608 от 29 апреля 1996 г.; Концепция национальной безопасности Российской Федерации, введенная Указом Президента РФ № 24 от 10 января 2000 г. Исходя из необходимости достижения целей обеспечения экономической безопасности предпринимательской деятельности, можно выделить следующие основные проблемные направления:

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

В современных рыночных условиях промышленность является самой наукоемкой отраслью, информация о которой является крайне дорогостоящей и требует особого подхода к защите данных от утечки. К тому же именно из данной отрасли развились конкурентная разведка и промышленный шпионаж. На сегодняшний день в области недобросовестной конкуренции выработаны разнообразные методы и приемы получения информации о производимой конкурентом продукции, противостоять которым достаточно сложно. Основная проблема обеспечения информационной безопасности в промышленных компаниях состоит в большой роли человеческого фактора в работе таких организаций. Доступ к разработкам имеет большое количество людей: доступ к информации о продукте, представляющей интерес для конкурента, может иметь как разработавший его инженер, так и простой рабочий. При этом, учитывая масштабы промышленных организаций, ограничить круг осведомленных лиц порой просто невозможно. Системы контроля утечки информации в такой ситуации становятся действительно незаменимыми. Если другие программные продукты занимаются задачей предотвращения в первую очередь внешних угроз, то DLP-системы, такие как SecureTower, ориентированы на защиту информации от утечки в результате инсайдерской активности. Для рассматриваемого предприятия необходимо определить место информационной безопасности в общей системе безопасности ООО «Белгородский завод «Энерготехмонтаж» (рис. 3.1.).

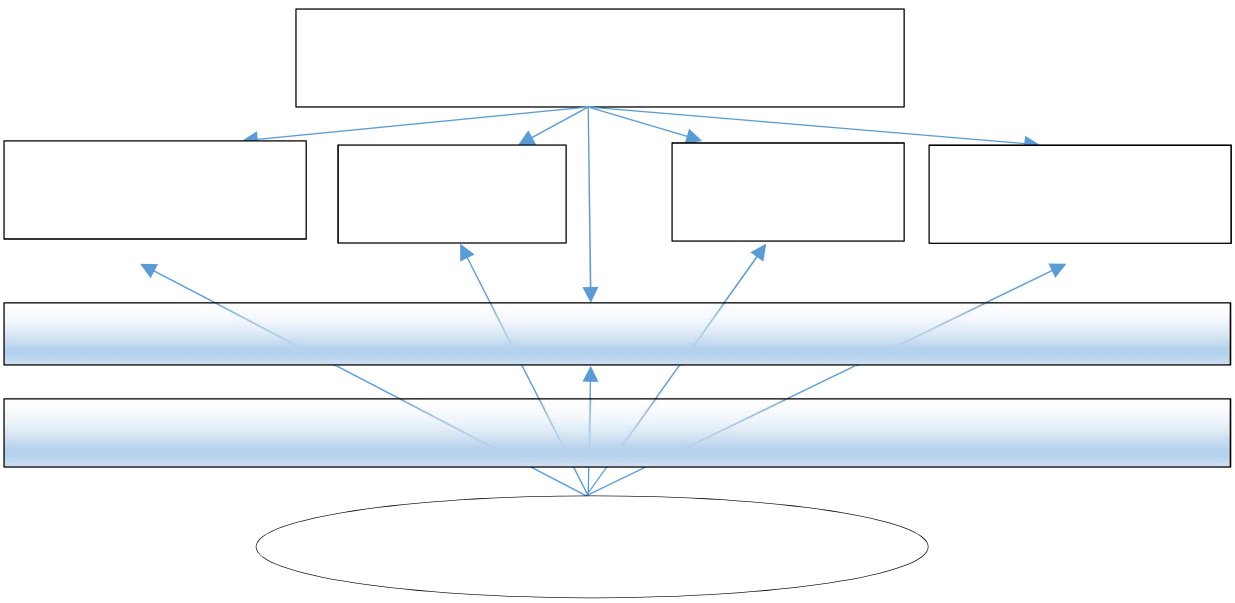


Рис. 3.1. Место информационной безопасности в общей системе безопасности ООО «Белгородский завод «Энерготехмонтаж»

В целях обеспечения безопасности коммерческой тайны в организации ООО «Белгородский завод «Энерготехмонтаж» предлагаем проект внедрения комплексной системы для предотвращения утечек информации и контроля активности сотрудников SecureTower.

SecureTower представляет собой комплексное программное решение для защиты бизнеса от внутренних угроз, функционал которого развивается в нескольких направлениях. Внедрение DLP-системы в корпоративную сеть является ключевым элементом при построении в организации эффективной системы управления информационной безопасностью. Информация, представляющая для бизнеса критическую важность, не должна покидать стен компании, а доступ к ней внутри организации должен быть ограничен. Для выполнения этих условий SecureTower анализирует весь внутренний и исходящий сетевой трафик организации. Более иллюстративно основные возможности программного решения представлены на рис. 3.2.

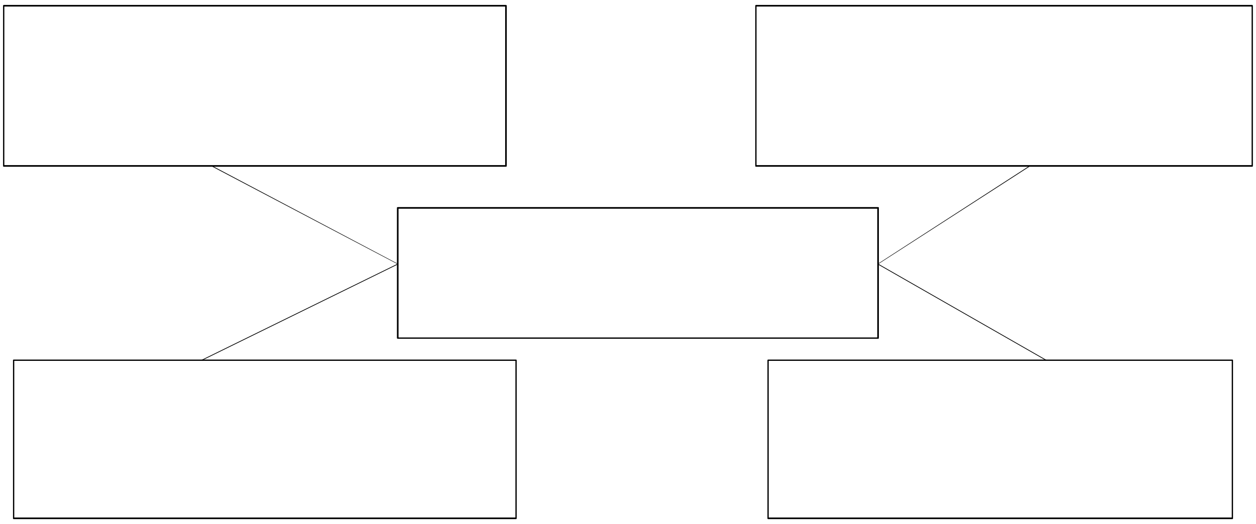


Рис. 3.2. Основные возможности программного решения SecureTower

Отметим, что данная программа имеет полный контроль всех каналов коммуникации: для превентивного устранения утечек и вредоносной инсайдерской активности в SecureTower реализован перехват максимально возможного количества каналов коммуникации. Это не только электронная почта, но и веб-активность, принтеры и USB-носители, а также мессенджеры и облачные сервисы. Возможности перехвата в SecureTower постоянно совершенствуются разработчиками, ориентируясь на пожелания заказчиков (рис. 3.3.).

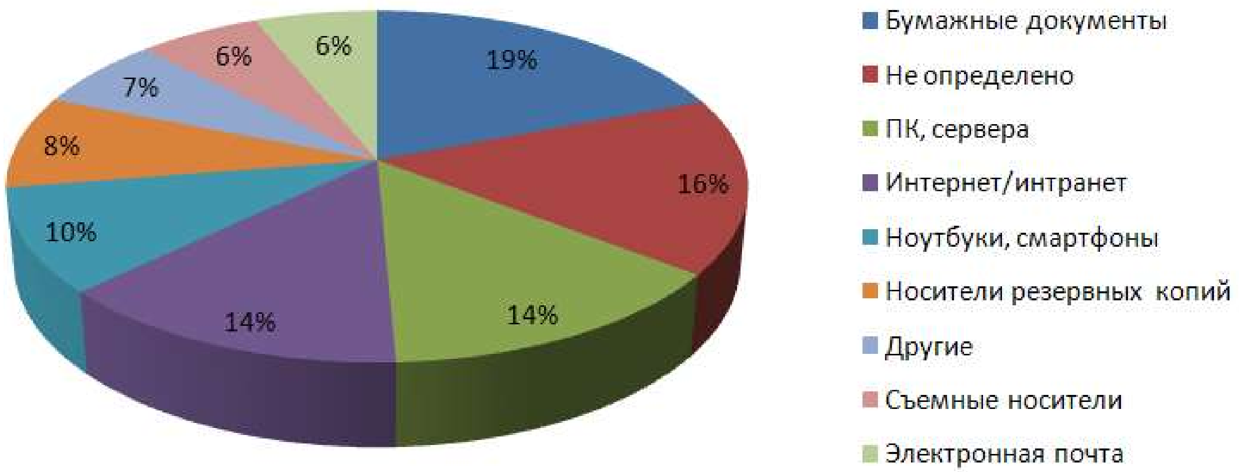


Рис. 3.3. Основные каналы утечек информации в 2016 году

При анализе информации SecureTower учитывает не только морфологические особенности языка, но также понимает текст, содержащий грамматические ошибки либо написанный транслитом. Кроме того, SecureTower умеет распознавать текстовую информацию на изображениях, файлах PDF и DjVu, анализирует формализованные данные, описываемые шаблонами (номера кредитных карт, ИНН, паспортные данные), и распознает печати в документах. Эти и многие другие возможности позволяют максимально эффективно защитить периметр организации от информационных утечек.

Подчеркнем, что в системе SecureTower полный контроль корпоративной информации достигается за счет мониторинга максимального числа коммуникационных каналов и протоколов передачи данных. Для обеспечения эффективной работы компании SecureTower полностью сохраняет всю деловую переписку персонала, по которой всегда доступен быстрый поиск. Кроме того, система контролирует время, которое сотрудник проводит в различных программах, сайтах и социальных сетях. Опираясь на эти данные можно настроить отправку уведомлений при повышении статистики посещения определенных сайтов, либо блокировать отдельные веб-ресурсы или программы. Основные возможные каналы утечки информации при ее обработке ЭВМ представлены на следующем рисунке.

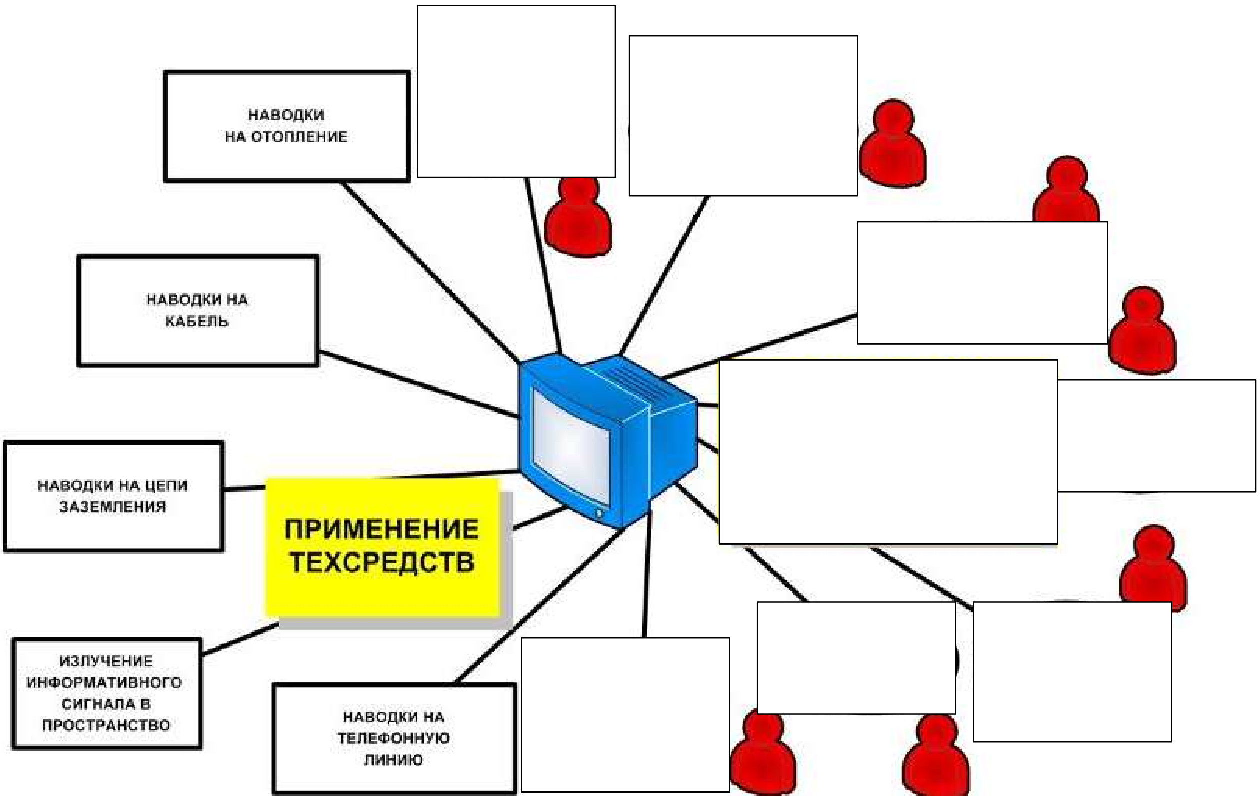


Рис. 3.4. Возможные каналы утечки информации при ее обработке ЭВМ

Следует отметить, что SecureTower эффективно и незаметно работает в сетях любой сложности, а также на предприятиях с территориально распределенной структурой. Внедрение, настройка и управление системой в таких организациях происходит централизованно – возможность из центрального офиса контролировать филиалы позволяет значительно снизить затраты службы безопасности на персонал.

Внедрение SecureTower занимает считанные часы, происходит незаметно и не загружает уже существующую сеть, а также не требует закупки дорогостоящего дополнительного оборудования. Возможны разные варианты использования системы: перехват с помощью программ-агентов на рабочих станциях, централизованный перехват с использованием зеркалирования трафика, интеграция с корпоративным сервером электронной почты и совместная работа с Proxy-устройством с помощью ICAP-интеграции.

На сегодняшний день современный бизнес практически полностью зависит от компетентности и ответственности сотрудников. Поэтому контроль персонала – это необходимость для любого предприятия. Руководителям нужно видеть полную картину рабочего дня, менеджмент должен корректировать команды и сроки, а служба безопасности – выявлять мошенников и нелояльных сотрудников.

Отметим, что 60% российских предприятий сталкиваются с внутрикорпоративной коррупцией (взятками, «откатами» и т.д.). Число преступлений по статье «мошенничество» растет с каждым годом. Контроль персонала значительно снизит риски экономических преступлений и утечек информации. Социальные сети и мессенджеры «съедают» весь рабочий процесс. Исключительно административными мерами выявить неэффективного работника долго и сложно – особенно среднего звена в крупных компаниях. Для того, чтобы оценить работу персонала (от целого филиала до отдельного сотрудника) – в SecureTower достаточно посмотреть автоматически генерируемый отчет. Сотрудник может плохо работать, потому что он находится в неподходящей команде. Анализ работы персонала позволит составить гораздо более эффективные рабочие команды. Знание о том, что твою работу контролируют – дисциплинирует и мотивирует.

В SecureTower полный контроль корпоративной информации достигается за счет мониторинга максимального числа коммуникационных каналов и протоколов передачи данных. Вся переписка автоматически анализируется и, в случае выявления нарушений, система мгновенной отправляет уведомление руководителю или службе безопасности.

SecureTower не позволит важной информации безвозвратно потеряться – все переданные и полученные данные сохраняются. Даже если удалить их с конкретной рабочей станции, они всё равно будут доступны и восстановлены в случае необходимости. Secure Tower контролирует максимальное количество каналов коммуникации, будь то электронная почта, мессенджеры, социальные сети, облачные хранилища, USB и другие – и сводит экономические и репутационные риски бизнеса к минимуму. SecureTower позволяет не только оперативно расследовать инциденты по горячим следам, но и своевременно предотвращать их. Заблокировав передачу данных определенного формата или запуск нежелательных процессов, SecureTower не допустит утечки критически важной для бизнеса информации.

Подчеркнем, что данным продуктом осуществляется полный контроль всех каналов коммуникации: для обеспечения максимальной защиты конфиденциальной информации SecureTower контролирует практически все каналы коммуникации и передачи данных (рис. 3.5.).

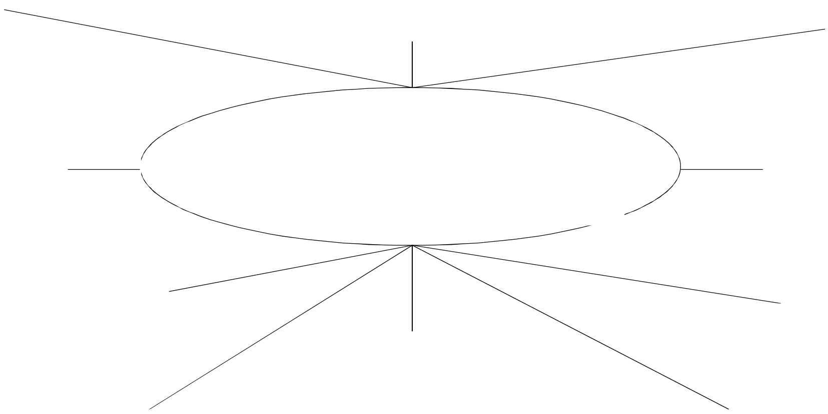


Рис. 3.5. Элементы контроля всех каналов коммуникации

Отметим более подробно следующие элементы контроля комуникаций: - электронная почта: SecureTower обеспечивает контроль всех сообщений большинства популярных почтовых серверов, по протоколам POP3, SMTP и IMAP, а также перехватывает и блокирует сообщения по протоколу MAPI. Система проверяет на соответствие политикам безопасности сообщения, переданные при помощи почтовых серверов Microsoft Exchange Server, Lotus Notes, Postfix, Sendmail и др. Кроме того, система поддерживает перехват сообщений внешних почтовых служб в бесплатных почтовых сервисах, таких как Gmail, Mail.ru или Яндекс.Почта;

- мессенджеры: сотрудники современных компаний все чаще переносят деловое общение из электронной почты в мессенджеры и социальные сети. Для контроля этих каналов в SecureTower реализован перехват сообщений и пересылаемых файлов в большинстве популярных мессенджеров. DLP-система может контролировать протоколы обмена мгновенными сообщениями OSCAR (ICQ/AIM), MMP (Mail.Ru Агент), XMPP (Jabber) (Miranda, Google Talk, QIP Infium, PSI), YIM (Yahoo! Messenger), SIP, а также перехватывать текстовые и голосовые сообщения и файлы в Skype, Viber, MS Lync и Telegram;

- социальные сети: помимо мессенджеров в деловом общении сотрудники все чаще используют социальные сети. SecureTower позволяет в автономном режиме перехватывать все сообщения в социальных сетях, таких как Вконтакте, Facebook, Одноклассники и другие. Также DLP-система контролирует общение сотрудников в блогах, онлайн-чатах, форумах и т.д.;

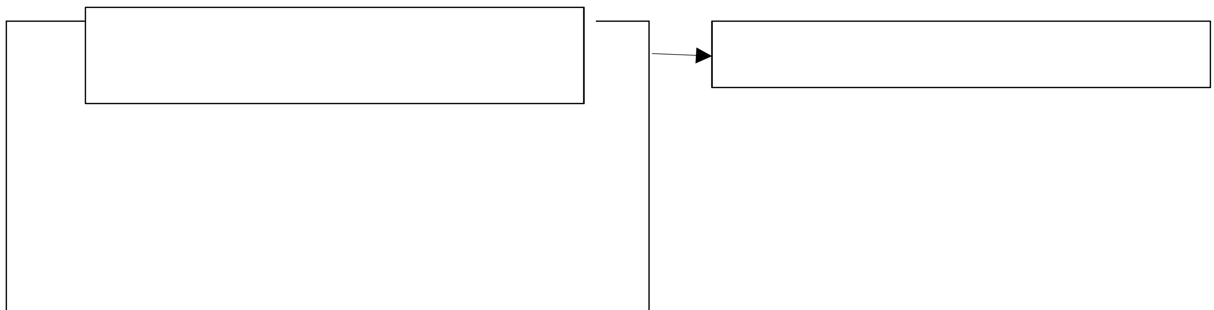
- Веб-активность: SecureTower позволяет составить полную картину веб-активности сотрудника в течение рабочего дня. С помощью DLP-системы можно узнать, какие сайты посещал работник, сколько времени на них проводил и оставлял ли там какие-либо сообщения;

- облачные хранилища: использование облачных хранилищ сотрудниками может быть как частью рабочего процесса, так и инцидентом безопасности. SecureTower отслеживает все файлы, загружаемые пользователем в интернет через браузер, а для таких облачных сервисов, как Dropbox, OneDrive и Яндекс.Диск, в системе также присутствует поддержка перехвата файлов в десктопных приложениях;
- приложения: DLP-система отслеживает, в каких приложениях работает сотрудник в течение рабочего дня. По итогам работы этого функционала можно посмотреть в диаграммах, какими приложениями работник пользовался чаще и какую часть времени уделил непосредственно трудовой деятельности. Кроме того, система позволяет блокировать запуск определенных, задаваемых администратором приложений;
- контроль сотрудников: одним из важнейших факторов при выборе DLP-системы является возможность контролировать работу сотрудников. Для этого в SecureTower реализован функционал для контроля рабочего времени, позволяющий увидеть, сколько реально времени работник потратил на выполнение той или иной задачи. Также благодаря кейлоггеру, функциям аудио- и видеомониторинга и снятия скриншотов рабочего стола можно составить полную картину рабочего дня сотрудника;
- контроль рабочих станций: SecureTower позволяет контролировать и предотвращать передачу файлов на внешние носители. Система автоматически сканирует отправляемые на печать или USB-устройство документы на наличие в них конфиденциальной информации, а в случае обнаружения таковой уведомляет администратора безопасности.

Кроме того, SecureTower отслеживает подключение и отключение устройств на рабочей станции, контролирует копирование информации и выполняет аудит доступа к компьютеру;

- индексирование рабочих станций: для проверки наличия либо отсутствия конфиденциальных документов на рабочей станции в SecureTower есть полноценный быстрый поиск по всем компьютерам в локальной сети, в том числе в ручном режиме. Поиск может выполняться как по именам, так и по атрибутам файлов;
- взаимосвязи персонала: для выявления взаимосвязей персонала в SecureTower используется граф-анализатор, в котором для каждого сотрудника система создает профайл, автоматически привязываемый к ActiveDirectory, и отображает его коммуникации с другими людьми. В этом профайле отображаются адреса электронной почты работника, имена в мессенджерах, аккаунты в социальных сетях и на других сайтах. Для выявления недоброжелателей вне компании SecureTower запоминает адреса внешних абонентов и также создает для них профайлы. Благодаря этому можно оперативно выявить внешнего злоумышленника или, например, рекрутера от конкурентов;
- отчёты: для сотрудников службы безопасности и руководителей структурных подразделений доступны полностью настраиваемые отчеты по инцидентам безопасности и ежедневной работе сотрудников. Также можно настроить автоматическое создание отчетов по расписанию и отправку их на электронную почту.

Гибкий инструмент для создания политики безопасности позволяет комбинировать разные методы контроля и создавать многокомпонентные правила, что минимизирует процент ложных срабатываний и повышает эффективность работы службы безопасности. Также хотелось бы отдельно подчеркнуть возможность программного продукта в контроле персонала и оптимизации бизнес-процессов, который включает в себя следующие составляющие (рис. 3.6).



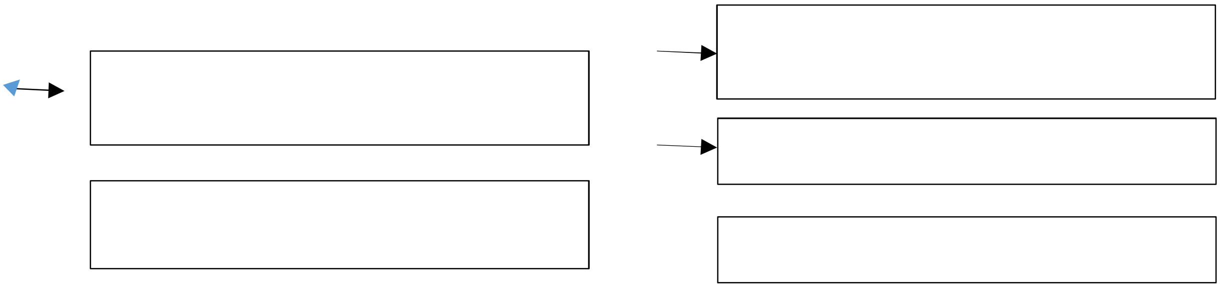


Рис. 3.6. Составляющие контроля персонала и оптимизации бизнес-процессов

Подчеркнем, что с помощью гибких правил система может блокировать передачу конфиденциальной информации и сообщать ответственному лицу об инциденте. Программный продукт позволит провести расследование инцидента в случае утечки: выявить нарушителей, определить в их действиях умысел, предпринять меры и выработать стратегию действий. Собранные данные могут приниматься судами в качестве доказательной базы. Что касается выявления нелояльных сотрудников, то здесь отметим следующее: программное решение дает возможность анализировать полную историю коммуникаций работников. С ее помощью возможно выявить абонентов по внешней сети, ведущих нежелательную активность, к примеру, пытающихся переманить ценные кадры или получить инсайдерскую информацию о предприятии. Также следует отметить, что контроль активности пользователя за ПК мотивирует персонал к большей ответственности. Руководство получает наглядную картину того, как сотрудник проводит рабочий день: сколько времени он активен, а сколько бездействует, с какими приложениями и как активно он работает, сколько времени проводит на различных сайтах.

Также сделаем акцент на следующий момент: статистические отчеты позволяют анализировать бизнес-процессы в компании и выявлять закономерности, которые указывают на нарушения принятых политик безопасности. Динамические отчеты по заданным критериям помогают оценить работу отдельных сотрудников и подразделений. Все отчеты интерактивны, что дает возможность перехода к просмотру событий и ускоряет расследование инцидентов. Отметим особенности графа-анализатора взаимосвязей персонала: он отслеживает контакты пользователей внутри организации и с внешними абонентами, в том числе с конкурентами. Такой инструмент позволяет выявить неформальных лидеров в коллективе, а также найти потенциальных инсайдеров в случаях, когда утечка конфиденциальной информации инициируется извне. Что касается фотографии рабочего дня, видео- и аудиозаписи, то здесь программный продукт формирует картину рабочего дня каждого сотрудника: руководство может оценить, насколько активно сотрудник использует каналы коммуникации. Кроме того, пользователь SecureTower может удаленно подключаться к веб-камере или рабочему столу сотрудника. Для расследования инцидентов и проверки активности сотрудника предусмотрена функция видео- и аудиозаписи. На вопрос: «Как SecureTower определяет, что пересылается конфиденциальный документ?» можно ответить следующим образом: технологии, используемые в SecureTower для анализа данных, сводят к минимуму ложные срабатывания системы на инциденты, связанные с нарушениями принятой в компании политики безопасности. Программа может проверять пересылаемые в сети документы по их атрибутам и содержанию, используя предварительно указанные ключевые слова с учетом морфологии. SecureTower также может проводить анализ на основании регулярных выражений для обнаружения отправки данных определенного вида, например, номера паспорта или кредитной карты. Кроме того, в программе используется технология цифровых отпечатков, которая работает следующим образом: система создает цифровые образы конфиденциальных документов, сохраняет их в базе данных, а затем сравнивает с каждым документом, пересылаемым в корпоративной сети. При любых совпадениях SecureTower отправляет уведомления о пересылке конфиденциального документа. Система также может делать цифровые отпечатки целых баз данных. Более того, пересылка конфиденциального документа или базы по электронной почте может быть заблокирована.

Несмотря на то, что основное предназначение функционала SecureTower заключается в защите корпоративных данных и обеспечении информационной безопасности на предприятии, система сыграет не последнюю роль в деле работы с бизнес-процессами. Используя данные из SecureTower можно привести к единому знаменателю время выполнения одних и тех же операций разными сотрудниками, выявить оптимальные алгоритмы работы целых отделов и определить среди персонала «слабое звено». Подчеркнем возможности использования SecureTower (рис. 3.7.).

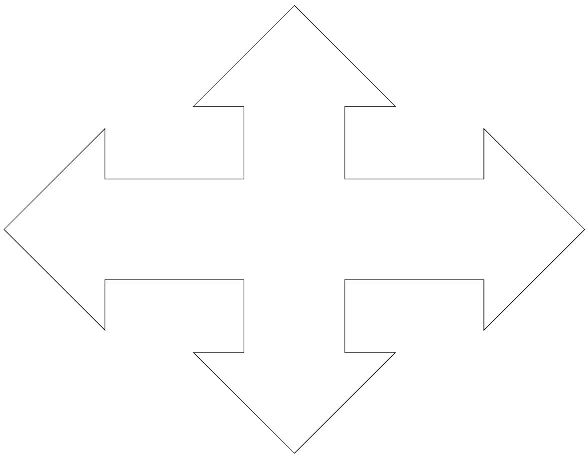
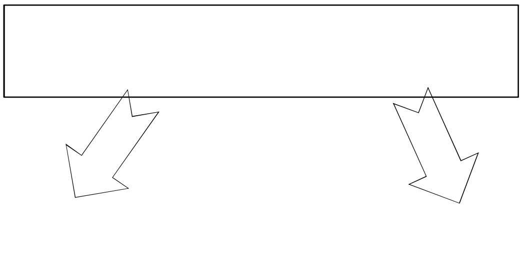


Рис. 3.7. Возможности использования SecureTower

Отметим, что программный продукт имеет гибкие настройки способов перехвата: пользователь может использовать несколько схем работы: перехват информации, установленными на компьютерах пользователей, централизованный перехват данных с использованием зеркалирования трафика или гибридный вариант, совмещающий оба способа. Рассмотрим систему разграничения прав доступа подробнее иллюстративно на рис. 3.8.



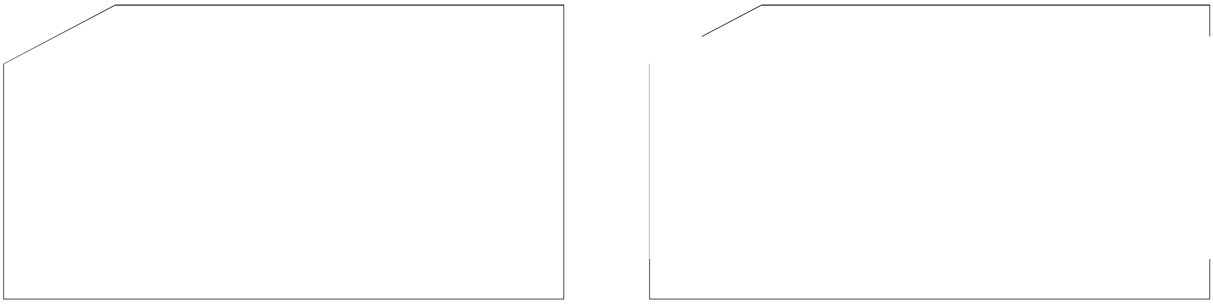


Рис. 3.8. Элементы системы разграничения прав доступа

Таким образом, в целях обеспечения безопасности коммерческой тайны в организации ООО «Энерготехмонтаж» по нашему мнению, проект внедрения комплексной системы для предотвращения утечек информации и контроля активности сотрудников SecureTower весьма актуален. SecureTower защищает интеллектуальную собственность, коммерческую и конфиденциальную информацию организации, контролирует лояльность персонала, целевое использование рабочего времени и оборудования. Фиксирует активность сотрудников в любых сервисах, приложениях, на сайтах и формирует детальные интерактивные отчеты. Также программный продукт контролирует максимально возможное количество каналов передачи данных , анализирует весь трафик на соответствие заданным правилам, блокирует передачу подозрительной информации и в автоматическом режиме уведомляет службу безопасности обо всех инцидентах. Система устанавливается в любую инфраструктуру сети, не требуя ее изменений, и функционирует незаметно для пользователя.

3.2. Проект комплексной защиты информации

Для реализации проекта внедрения комплексной системы для предотвращения утечек информации и контроля активности сотрудников ООО «Белгородский завод «Энерготехмонтаж», необходимо приобрести лицензию на программное обеспечение SecureTower. Данный программный продукт предлагает московская компания «Falcongaze»: с 2007 года занимается разработкой программного обеспечения в сфере информационной безопасности. Флагманский продукт компании – комплексное решение SecureTower, предназначенное для предотвращения утечек информации и мониторинга деятельности сотрудников. В Белгороде находится партнер указанной фирмы – системный интегратор ООО «Радиус». Для начала, необходимо определиться с инвестиционными вложениями (единовременные затраты) в реализацию проекта информационной безопасности. Рассмотрим в таб. 3.1 прайс FalconGaze SecureTower для контроля 50 пользователей в пределах одной сети.

Таблица 3.1

Прайс «FalconGaze» SecureTower для контроля пользователей в пределах одной сети:

№	Товары (работы, услуги)	Кол-во	Ед.	Цена/Без НДС*	Сумма/ Без НДС
1	Лицензия на программное обеспечение «Falcongaze SecureTower»	35	шт	4 875	170 625
2	Серверные компоненты	3	шт	50	150 000
Итого:					320 625

Иллюстративно диаграмма инвестиционных затрат представлена на рис. 3.9.

Рис. 3.9. Инвестиционные затраты ООО «Энерготехмонтаж»

Согласно подпункту 26 пункта 2 статьи 149 Налогового кодекса Российской Федерации предоставление прав на использование программ для ЭВМ по Лицензионному договору не облагается налогом на добавленную стоимость. Срок поставки продукта составляет 5 (пять) рабочих дней после оплаты. Условия оплаты: авансовый платеж. SecureTower лицензируется как помодульно, так и по количеству контролируемых пользователей. Минимальная лицензия включает в себя возможность перехвата данных от 25 пользователей по всем каналам связи и протоколам. При покупке SecureTower можно свободно варьировать количество контролируемых протоколов и пользователей в лицензии. Для установки SecureTower необходимо наличие прав администратора на локальном сервере, а также на удаленных компьютерах, куда будут установлены агенты. Если такие права есть, то системного администратора уведомлять не нужно. Благодаря этому специалисты отдела информационной безопасности имеют возможность контролировать деятельность всех сотрудников, в том числе и системных администраторов, на предмет соблюдения корпоративной политики. В стоимость лицензии входит годовое бесплатное сопровождение, включающее в себя техническую поддержку и возможность получения заказчиком бесплатно новых версий «Falcongaze SecureTower», бессрочная лицензия на 35 компьютеров, 2 года доступа к обновлениям, 2 года стандартной технической поддержки. В последующие года предприятие ООО «Белгородский завод «Энерготехмонтаж» должно оплачивать только 25 % за ведение и обновление программного продукта от общей стоимости лицензии (в первый год реализации проекта внедрения комплексной системы для предотвращения утечек информации и контроля активности сотрудников «Энерготехмонтаж» стоимость уже включена в лицензию за 35 компьютеров) (табл. 3.2).

Таблица 3.2

Постоянные затраты на обслуживание и техническую поддержку

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	42 656	42 656
Всего	0	42 656	42 656

На основании табл. 3.2 мы видим, что только статья затрат «обслуживание и техническая поддержка» составляют постоянные расходы. Иллюстративно постоянные затраты представлены на следующем рисунке.

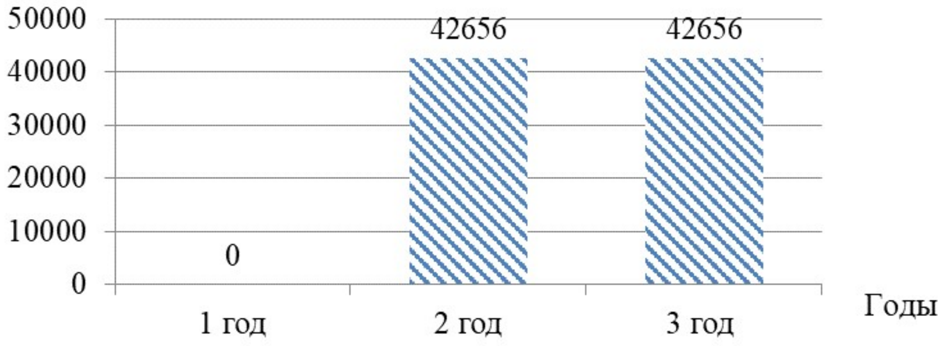


Рис. 3.9. Постоянные затраты ООО «Энерготехмонтаж»

Переменные расходы в данном проекте не предусмотрены. Подчеркнем, что программный продукт обладает простотой внедрения – нет необходимости закупать дорогостоящее оборудование и вызывать специалиста, установка занимает совсем немного времени. Интерфейс понятный, эффективно работает в сетях любой сложности. Сопровождение проводится на всех этапах: поддержка, обучение, консалтинг и сертификация персонала.

SecureTower характеризуется комплексностью, один продукт решает целый спектр задач: предотвращение утечек информации, мониторинг работы сотрудников, ведение архива бизнес коммуникаций.

SecureTower поддерживает работу в компаниях с территориально распределенной структурой офисов. Программа позволяет контролировать различные каналы связи, а также осуществлять мониторинг деятельности сотрудников, используя удаленный доступ к нескольким ресурсам или объединяя все анализируемые данные в единое централизованное хранилище.

Внедрение нового программного продукта характеризуется большим количеством положительных возможностей для рассматриваемой организации. Также внедрение нового программного решения позволит снизить затраты ориентировочно на 8%. Экономическую эффективность проекта внедрения комплексной системы для предотвращения утечек информации и контроля активности сотрудников ООО «Белгородский завод «Энерготехмонтаж» можно оценить с помощью экономии денежных средств.

Рассматривая затраты предприятия за 2017 год, проведем расчет экономии денежных средств в таблице 3.3.

Таблица 3.3

Расчет экономии денежных средств, руб.

Показатель	1 г.	2 г.	3 г.
Затраты до внедрения программного продукта, тыс. руб.	1 666 563	1 999 876	2 439 848
Затраты после внедрения программного продукта, тыс. руб.	1 533 238	1 839 886	2 244 661
Экономия, тыс. руб.	133 325	159 990	195 188

Отметим, что затраты до внедрения программного продукта предприятия в 2019-2010 гг. представлены на основании оперативных данных предприятия (в 2019 году по данным предприятия затраты увеличатся на 20 %, в 2020 году – на 22 %). Более иллюстративно экономия затрат представлена на рис. 3.10.

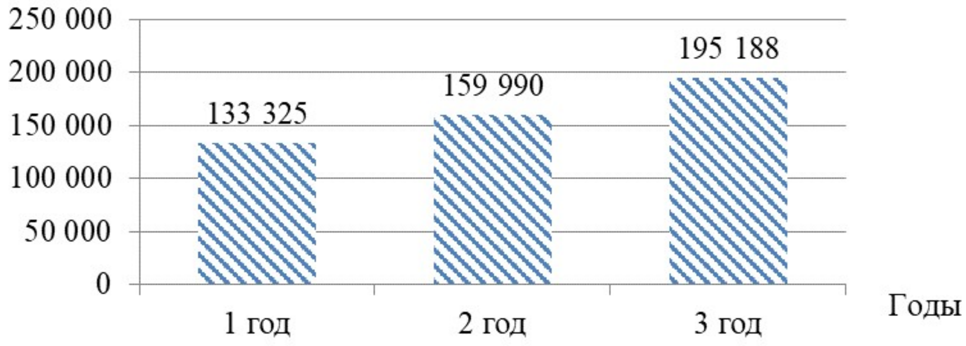


Рис. 3.10. Экономия затрат ООО «Энерготехмонтаж»

Мы наблюдаем прогнозируемую экономию затрат за счет внедрения программного продукта «SecureTower». Конечно, внедрение данного программного решения совершенно недорогостоящее для такого предприятия, прогнозируется существенная экономия денежных средств и на основании представленного можно провести расчет денежных потоков (табл. 3.4).

Таблица 3.4

Расчет денежных потоков, руб.

Наименование показателя	0 г.	1 г.	2 г.	3 г.
Экономия, тыс. руб.	0	133 325	159 990	195 188
Инвестиционные затраты, руб.	- 320 625	0	0	0
Постоянные затраты, руб.	0	0	42 656	42 656
Себестоимость, руб.	0	0	42 656	42 656
Экономический эффект, тыс. руб.	0	133325, 000	151947,344	195145,344
Чистый денежный поток, руб.	- 320 625	133325 000	151947344	195145344
Чистый денежный поток нарастающим итогом, руб.	- 320 625	133004375	248951719	444097000

На основании представленных данных в табл. 3.4 наблюдается положительная тенденция роста чистого денежного потока (рис. 3.11).

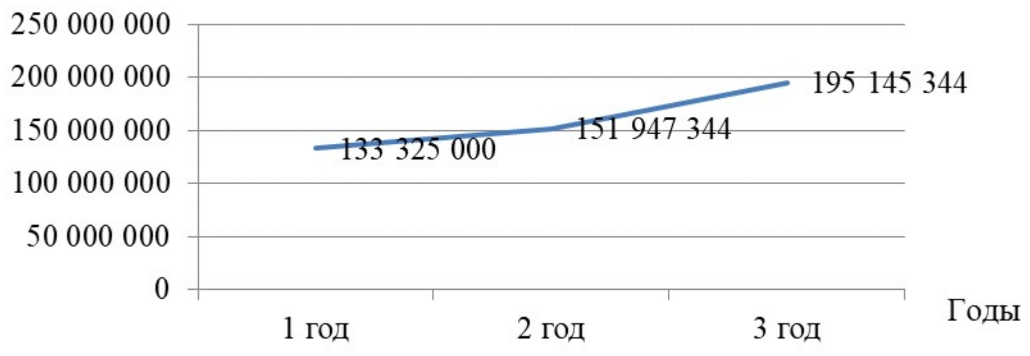


Рис. 3.11. Чистый денежный поток ООО «Энерготехмонтаж»

Зная чистый денежный поток и чистый денежный поток нарастающим итогом, следует рассчитать чистую современную стоимость, индекс рентабельности, срок окупаемости, дисконтированный срок окупаемости проекта.

Отметим, что чистая современная стоимость – это чистая текущая стоимость - сумма текущих стоимостей всех прогнозированных, с учетом ставки дисконтирования, денежных потоков. Если данный показатель NPV > 0, то инвестиционные затраты увеличат капитал фирмы 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 NPV проекта на основании следующих данных: чистых денежных потоков; денежного потока нарастающим итогом; ставки дисконтирования. В таблице 3.9 приведен расчет чистой современной стоимости (NPV) проекта.

Таблица 3.9

Расчет NPV проекта, руб.

Показатель	0	1	2	3
Чистый денежный поток	- 320 625	133 325 000	151 947 344	195 145 344
Чистый денежный поток нарастающим итогом (аккумулированный денежный поток)	- 320 625	133 004 375	248 951 719	444 097 000

Ставка дисконтирования, %	-	20	20	20
Коэффициент дисконтирования	1	0,833	0,694	0,578
Дисконтированный денежный поток	- 320 625	111 099 723	105 451 457	112 794 009
Дисконтированный денежный поток нарастающим итогом (Аккумулированный дисконтированный денежный поток)	- 320 625	110 779 098	216 230 555	329 024 564

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; дисконтирование денежных потоков – это приведение стоимости потоков платежей, выполненных в разные моменты времени, к стоимости на текущий момент времени.

Чистая современная стоимость (NPV) составит: - 320 625 + 111 099 723 + 105 451 457 + 112 794 009 = 329 024 564 руб. Что касается индекса рентабельности, то его значение составляет 1026 руб. Индекс рентабельности больше 1, значит проект следует принять к реализации.

SecureTower обеспечивает полный контроль документооборота и позволяет вовремя предупредить утечку конфиденциальной информации. Под наблюдением системы находятся все информационные каналы, от электронной почты до мессенджеров и USB-устройств. Контроль за информацией и предотвращение утечек являются основными задачами, стоящими перед DLP-системой. В SecureTower они решаются с помощью самого действенного инструментария: перехват всех отправляемых и получаемых сообщений, выявление отправки конфиденциальных документов, контроль принтеров и подключаемых устройств, контроль почтовых серверов, гибкая система создания правил безопасности и многое другое. Наряду с другими инструментами для обеспечения безопасности в SecureTower используется технология выявления передачи конфиденциальной информации по цифровым отпечаткам. Для этого производится анализ документов, которые требуется контролировать, а после в информационном потоке выявляются совпадения (даже фрагментарные) с этими документами.

Представим возможные угрозы до и после предлагаемого проекта в следующей таблице.

Таблица 3.10

Угрозы до и после предлагаемого проекта

Угроза до внедрения проекта	Угроза после внедрения проекта
Рабочее место сотрудника	
1. Физический доступ нарушителя к рабочему месту	1.Контроль за рабочим местом
2. Разрушение (повреждение, утрата) конфиденциальной информации при помощи специализированных программ и вирусов	Отсутствие возможности разрушения (повреждение, утрата) конфиденциальной информации при помощи специализированных программ и вирусов
Конфиденциальная информация	
1.Физический доступ нарушителя к носителям	Контроль за рабочим местом
2. Несанкционированное копирование, печать и размножение носителей конфиденциальной информации	Контроль за доступом сотрудников к копировальной и множительной технике

Далее представим структуры многоуровневой системы безопасности бизнеса.

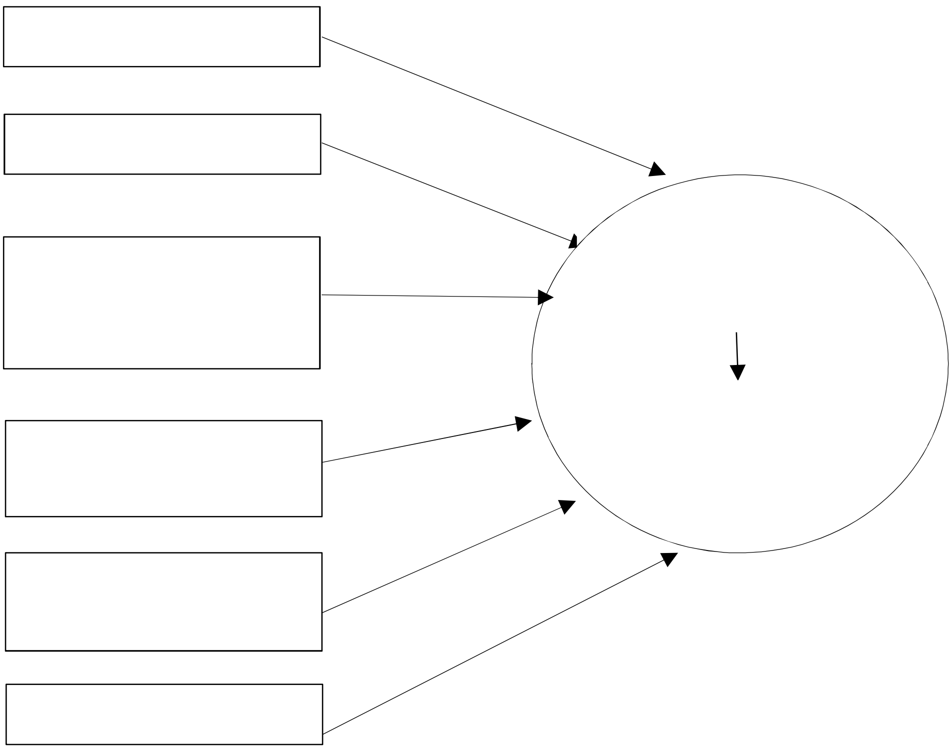


Рис. 3.12. Структура многоуровневой системы безопасности бизнеса

Новый программный продукт позволит исследуемому предприятию работать на следующих принципах обеспечения информационной безопасности (рис. 3.13).

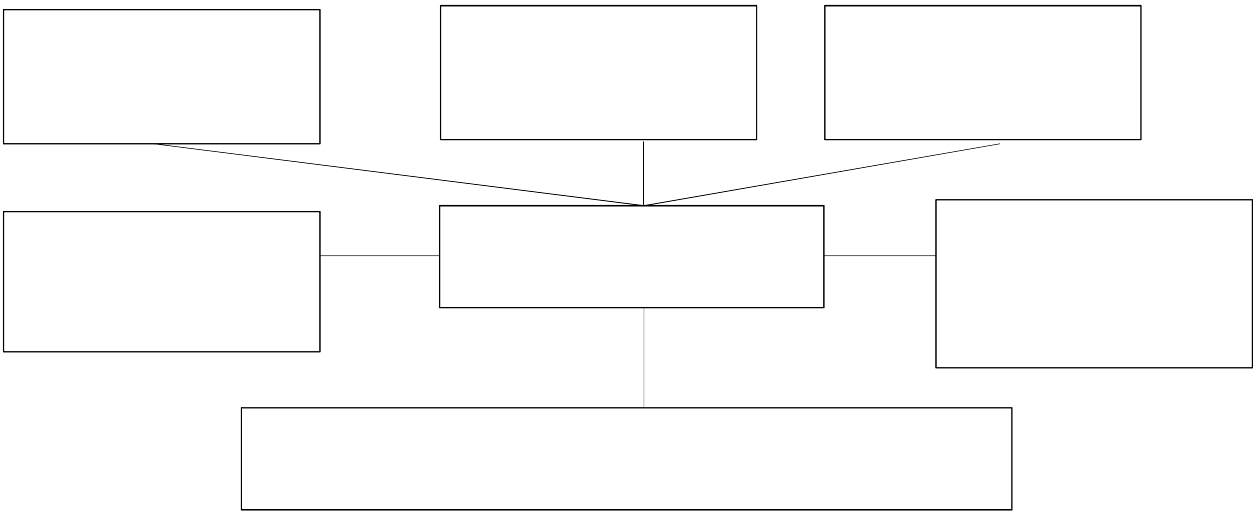


Рис. 3.14. Принципы обеспечения информационной безопасности

Таким образом, в целях обеспечения безопасности коммерческой тайны в организации ООО «Белгородский завод «Энерготехмонтаж» нами был предложен проект внедрения комплексной системы для предотвращения утечек информации и контроля активности сотрудников SecureTower. SecureTower представляет собой комплексное программное решение для защиты бизнеса от внутренних угроз, функционал которого развивается в нескольких направлениях. Внедрение DLP-системы в корпоративную сеть является ключевым элементом при построении в организации эффективной системы управления информационной безопасностью. В рамках произведенных расчетов наблюдаем прогнозируемую экономию затрат за счет внедрения программного продукта «SecureTower». 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 8%.

ЗАКЛЮЧЕНИЕ

Таким образом, в выпускной квалификационной работе были решены следующие задачи:

1. Представлены теоретико-методологические основы защиты информации:

- рассмотрено содержание и принципы защиты информации на предприятии;

- представлена классификация угроз безопасности информации;

- рассмотрены способы защиты информации на предприятии.

2. Проанализированы основные критерии экономической безопасности ООО «БЕЛГОРОДСКИЙ ЗАВОД «ЭНЕРГОТЕХМОНТАЖ»:

- рассмотрена организационно-экономическая характеристика предприятия;

- проанализированы показатели финансово-хозяйственной деятельности;

- проанализирована система защиты информации на предприятии.

3. Разработана система мер по обеспечению защиты информации на предприятии ООО «БЕЛГОРОДСКИЙ ЗАВОД «ЭНЕРГОТЕХМОНТАЖ»:

- предложены основные направления по совершенствованию защиты информации;

- разработан проект комплексной защиты информации.

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

В данной работе объект исследования - ООО «Белгородский завод «Энерготехмонтаж»». Предприятие является разработчиком и производителем широкой номенклатуры высоковольтного и низковольтного оборудования. Вся номенклатура выпускаемой продукции имеет сертификаты соответствия качеству, находится по адресу: 308017 г. Белгород, ул. Константина Заслонова, 175-а. В перспективе планируется расширение производства путем внедрения оборудования на элегазовом выключателе, организации отдельного структурного подразделения для проведения электромонтажных работ в полном объеме: электротехническая лаборатория, организация пуско-наладочных работ и пр. Ведется работа по организации участка для гальванической обработки металла и участка аргонно-дуговой сварки для работы с электрошиной. Рассматривая динамику показателей финансово - хозяйственной деятельности ООО «Белгородский завод «Энерготехмонтаж»» особое внимание следует обратить на рентабельность чистых активов и средневзвешенную стоимость капитала. Для успешного развития деятельности необходимо, чтобы рентабельность чистых активов была выше средневзвешенной стоимости капитала, тогда предприятие способно выплатить не только проценты по кредитам и объявленные дивиденды, но и реинвестировать часть чистой прибыли в производство. Изменение за анализируемый период структуры пассивов следует признать в подавляющей части негативным.

Коэффициент абсолютной ликвидности и на начало и на конец анализируемого периода (31.12.2015 г. - 31.12.2017 г.) находится ниже нормативного значения (0,2), что говорит о том, что значение коэффициента слишком низко и предприятие не в полной мере обеспечено средствами для своевременного погашения наиболее срочных обязательств за счет наиболее ликвидных активов. На начало анализируемого периода - на 31.12.2017 г. значение показателя абсолютной ликвидности составило 0,09. На конец анализируемого периода значение показателя снизилось, составив 0,01.

Коэффициент промежуточной (быстрой) ликвидности показывает, какая часть краткосрочной задолженности может быть погашена за счет наиболее ликвидных и быстро реализуемых активов. Нормативное значение показателя - 0,6-0,8, означающее, что текущие обязательства должны покрываться на 60-80% за счет быстрореализуемых активов. На начало анализируемого периода (на 31.12.2015 г.), значение показателя быстрой (промежуточной) ликвидности составило 0,75. На 31.12.2017 г. значение показателя снизилось, что можно рассматривать как отрицательную тенденцию, и составило 0,61.

Коэффициент текущей ликвидности и на начало и на конец анализируемого периода (31.12.2015 г. - 31.12.2017 г.) находится ниже нормативного значения 2, что говорит о том, что значение коэффициента достаточно низкое и предприятие не в полной мере обеспечено собственными средствами для ведения хозяйственной деятельности и своевременного погашения срочных обязательств.

Рассматривая показатели рентабельности, прежде всего следует отметить, что и на начало, и на конец анализируемого периода частное от деления прибыли до налогообложения и выручки от реализации (показатель общей рентабельности) находится у ООО «Белгородский завод «Энерготехмонтаж»» ниже среднеотраслевого значения, установившегося на уровне 10%.

За анализируемый период значения большинства показателей рентабельности увеличились, что следует скорее рассматривать как положительную тенденцию. В настоящее время вероятность банкротства предприятия можно оценить как низкую.

Анализируя систему защиты информации на предприятии, можно сделать вывод, что конкретная служба по защите информации в ООО «Белгородский завод «Энерготехмонтаж»» отсутствует. Поэтому ответственность за защищаемую информацию несет специалист по управлению персоналом. Данная документация обрабатываются путем строгого контроля изъятия и возвращения документов под расписку уполномоченного работника. За информацию, относящуюся к коммерческой тайне, несут ответственность следующие служащие предприятия: начальники, бухгалтера, экономисты, инженеры. Безопасность информации ООО «Белгородский завод «Энерготехмонтаж»» - 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. В целях обеспечения безопасности коммерческой тайны в организации ООО «Белгородский завод «Энерготехмонтаж» предлагаем проект внедрения комплексной системы для предотвращения утечек информации и контроля активности сотрудников SecureTower. SecureTower представляет собой комплексное программное решение для защиты бизнеса от внутренних угроз, функционал которого развивается в нескольких направлениях. в целях обеспечения безопасности коммерческой тайны в организации ООО «Белгородский завод «Энерготехмонтаж» нами был предложен проект внедрения комплексной системы для предотвращения утечек информации и контроля активности сотрудников SecureTower. SecureTower представляет собой комплексное программное решение для защиты бизнеса от внутренних угроз, функционал которого развивается в нескольких направлениях. Внедрение DLP-системы в корпоративную сеть является ключевым элементом при построении в организации эффективной системы управления информационной безопасностью. В рамках произведенных расчетов наблюдаем прогнозируемую экономию затрат за счет внедрения программного продукта «SecureTower». 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 8%.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

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

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

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

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

5. Абалкин, Л. Экономическая безопасность России: угрозы и их отражение / Л. Абалкин // Вопросы экономики. - 2015. - № 12. - С. 48-59.

6. Абдурахманов, А. А. Современные подходы к организации мониторинга криминологической ситуации в регионе / А.А. Абдурахманов //Право и политика. – 2011. - №6.

7. Аганбегян, А.Г. Социально - экономическое развитие России [Текст] / А.Г. Аганбегян. - Академия народного хозяйства при Правительстве РФ. - 2- е изд., испр. и доп. - 2015. - 374 с.

8. Аликперов, И. М. Социально-экономические основы экономической безопасности / И.М. Аликперов // Вестник института цивилизации. - 2014. - №1.

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

10. 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

11. Вихорев, С. Как определить источники угроз / С. Вихорев, Р.Кобцев //Открытые системы. - 2014. - №07-08.-С.43.

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

13. Галатенко, В.А. Основы информационной безопасности. - М.: Интуит, 2014. – 340 с.

14. Гмурман, А.И. Информационная безопасность/ А.И. Гмурман - М.: «БИТ-М», 2014.-387с.

15. Дъяченко, С.И. Правовые аспекты работы в ЛВС/ С.И. ДъяченкоСПб.: «АСТ», 2016.- 234с.

16. Домарев В.В., – Безопасность информационных технологий. Персональный сайт к.т.н. Домарева В.В. [Электронный ресурс] – Режим доступа: http://www.security.ukrnet.net/modules/news/

17. Завгородний, В.И. Комплексная защита информации в компьютерных системах. - М.: Логос, 2014. – 410 с.

18. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда. - М.: Интуит, 2016. – 300 с.

19. Зима, В. Безопасность глобальных сетевых технологий / В.Зима, А. Молдовян, Н. Молдовян - СПб.: BHV, 2014. - 320 с.

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

21. Коржов, В. Стратегия и тактика защиты / В.Коржов //Computerworld Россия.- 2014.-№14.-С.26.

22. Каранина, Е.В. Формирование и обеспечение финансовоэкономической безопасности на основе критериев риск-

системы: комплексный подход: монография / Е.В. Каранина. - Киров: Типография «Старая Вятка», 2015.– 400с.

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

24. Любецкий, Р. В. Совершенствование институциональной системы формирования человеческого капитала в современной России / Р.В. Любецкий: дис. ... канд. экон. наук. М., 2014. – 520 с.

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

26. Лыкин, С. Развитие экономики России и ее структуризация как гарантия экономической безопасности // Вопросы экономики. – № 12. – 2013– С. 45-51.

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

28. 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.

29. 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

30. Острейковский, В.А. Информатика: Учеб. пособие для студ. сред. проф. учеб. Заведений/ В.А. Острейковский- М.: Высш. шк., 2014. - 319с.:ил.

31. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. / Петренко С.А., Симонов С.В. – М.: Компания АйТи ; ДМК Пресс, 2014. – 384 с.: ил.

32. Петренко С.А. Методика построения корпоративной системы зашиты информации. [Электронный ресурс]: http://www.myportal.ru/scc/doc24.html

33. Селина Н.В., – Исследование эффективности защищенности корпоративных систем средствами и методами визуального моделирования. [Электронный ресурс] – Режим доступа: http://masters.donntu.org/2010/ fknt/selina/diss/index.htm

34. Семенов, Г. Цифровая подпись. Эллиптические кривые / Г.Семенов // Открытые системы.- 2014. - №07-08. - С.67-68.

35. Титоренко, Г.А. Информационные технологии управления/ Г.А. Титоренко - М.: Юнити, 2016.-376с.

36. Устинов, Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий/ Г.Н. Устинов- М.: Радио и связь, 2016.342с.

37. Фомин, А. Экономическая безопасность [Электронный ресурс] / А. Фомин / Режим доступа: http://www.intertrends.ru/twenty-four/012.htm

38. Химка С.С., – Разработка моделей и методов для создания системы информационной безопасности корпоративной сети предприятия с учетом различных критериев. [Электронный ресурс] – Режим доступа: http://masters.donntu.org/2016/fvti/khimka/diss/index.htm

39. Цикра Р.С. Исследование и разработка методов повышения достоверности передачи информации в корпоративной сети промышленного предприятия. [Электронный ресурс] – Режим доступа: http://masters.donntu.org/2016/kita/tsikra/diss/index.htm

40. Цымбалова А.А., – Разработка модели использования и распределение ресурсов, выделяемых на защиту информации. [Электронный ресурс] – Режим доступа: http://www.masters.donntu.org/2011/fknt/tsymbalova /diss/index.htm

41. Шахраманьян, М.А. Новые информационные технологии в задачах обеспечения национальной безопасности России/ Шахраманьян, М.А. - М.: ФЦ ВНИИ ГОЧС, 2016.- 222с.

42. Шершенев, Л. И. Безопасность: государственные и общественные устои / Л. И. Шершенев// Безопасность. – № 4. (20). – 2014 г. – С. 12-13.

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

44. Экономическая информатика / под ред. П.В. Конюховского и Д.Н. Колесова. - СПб.: Питер, 2016. - 560с.:ил.

45. Экономическая безопасность России: Общий курс: учебник / под ред. В. К. Сенчагова. - 2-е изд. - М., 2015. – 400 с.

46. Экономическая и национальная безопасность: учеб. / Под ред. Е.А. Олейникова. - М.: Экзамен, 2014. - 287 с.

47. Экономическая безопасность: теория, методология, практика / под науч. ред. Никитенко П.Г., Булавко В. Г.; Институт экономики НАН Беларуси. - Минск: Право и экономика, 2013. - 394 с.

48. Экономическая безопасность: Общий курс. Учебник. Изд. 4-е. / Под ред. В.К. Сенчагова - М.: Дело, 2012. - 304 с.

49. Экономическая безопасность: Производство - Финансы - Банки. / Под ред. В.К. Сенчагова - М.: ЗАО «Финстатинформ», 2012. - 400 с.

50. Экономическое развитие России и мировые тенденции на рубеже веков/ под. ред. Никомова А.К. - М.: Институт США РАН, 2012. - 510 с.

ПРИЛОЖЕНИЯ