МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

Кафедра Экономики, управления и права

Система противодействий угрозам имущественной безопасности со стороны персонала

Магистерская диссертация
по направлению: 38.04.02 Менеджмент
Профильная направленность: «Управление человеческим капиталом»

Проверка на объем заимствований:
47,90 % авторского текста

Работа рекомендована к защите
«11» 12 2020 г.
Зав. кафедрой Э,У и П
(Рябчук Павел Георгиевич)

Выполнила:
Студентка группы ЗФ-309-147-2-2
Мезенцева Анастасия Сергеевна

Научный руководитель:
Доктор педагогических наук, профессор
Саламатов А.А.

Челябинск, 2020

Содержание

Введение

Система защиты имущества предприятии должна строиться по определенным принципам. Это обусловлено необходимостью противодействия целому ряду угроз безопасности имущества.

Основным принципом противодействия угрозам безопасности имущества, является превентивность принимаемых мер защиты, так как устранение последствий проявления угроз требует значительных финансовых, временных и материальных затрат.

В настоящее время актуален вопрос защиты имущества предприятия от собственных недобросовестных сотрудников предприятия.

Актуальность темы исследования состоит в том, что всё чаще возникают случаи, когда главной опасностью для собственности предприятия становится внутренний нарушитель - собственный сотрудник, получивший неограниченный доступ к имуществу предприятия в пределах своей компетенции.

К категориям работников, имеющим доступ к денежным ресурсам (в том числе с помощью IT), и могущими быть потенциальными источниками её разглашения, либо иных неправомерных действий, относятся, прежде всего, работники бухгалтерии, кассиры, лица, имеющие право распоряжения печатями, бланками, работники компьютерных подразделений.

Недобросовестные сотрудники – это категория служащих, которые наносят ущерб предприятию, преследуя самые разнообразные цели личного характера. В частности, получение крупных вознаграждений от контрагентов, месть, торговля секретами предприятия как источник дополнительного заработка и др.

Нанесение ими ущерба выражается в следующих формах: кража или порча имущества, разглашение или перепродажа коммерческой тайны, выведение из строя технических средств связи и вычислительной техники, заражение ЭВМ компьютерными вирусами, невыполнение своих функциональных обязанностей.

Также часты случаи утечки информации из-за халатности сотрудников и перегруженности их работой.

Успешное функционирование организации в условиях рыночной экономики предполагает обеспечение эффективной системы мер безопасности, в том числе информационной. Экономика становится более информационно насыщенной, вопрос качественного доступа к информационным ресурсам выходит на одно из первых мест в конкурентной борьбе. Соответственно, обеспечение информационной безопасности становится ключевым фактором достижения конкурентоспособности организации.

Персонал организации влияет на все аспекты ее жизнедеятельности, а также неразрывно связан с ее информационной и экономической безопасностью. Возрастание роли угроз информационной безопасности со стороны собственного персонала в современных условиях обусловлено, с одной стороны, такими социальными тенденциями, как либерализация экономики и рынка труда; изменение сущности контроля за персоналом; повышение роли менеджмента персонала в управлении организацией; с другой стороны, в это время наблюдаются процессы усложнения труда, роли творчества и инноваций, предоставление работникам свободы и автономии в принятии решений, что приводит к ослаблению возможности жесткого контроля за персоналом.

Не смотря на довольно широкий спектр мероприятий, разработанных в последние время и направленных на предупреждению угроз имущественной безопасности предприятия, ежегодные потери от намеренных действия персонала не показывает динамики к снижению. Таким образом, для предприятий в условиях современного рынка остается открытым и актуальным вопрос обеспечения имущественной безопасности.

Цель исследования: произвести апробацию эффективности практического обеспечения информационной безопасности от угроз со стороны собственного персонала в организации ООО «Вектор» и разработка рекомендаций по ее совершенствованию;

Для достижения поставленной цели выпускной квалификационной работы представляется необходимым обеспечить решение следующих ***задач исследования***:

- Выявить научное значение понятия конфиденциальной информации и возникновения потенциальных угроз со стороны конкурентного сегмента (позициям) организации в случае ее разглашения;
- определить ключевые (факторные) угрозы информационной безопасности организации, исходящие от ее безответственных и нелояльных сотрудников;
- Охарактеризовать ООО «Вектор» и провести факторный анализ динамики его кадрового потенциала за исследуемый период 2018-2019 гг.
- проанализировать практику обеспечения защиты конфиденциальной информации от угроз со стороны безответственных и нелояльных сотрудников и выявленные в ней недостатки;
- разработать рекомендации по совершенствованию практики защиты конфиденциальной информации в электронной форме;
- разработать рекомендации по совершенствованию практики защиты конфиденциальной информации на печатных носителях;
- разработать рекомендации по совершенствованию практики защиты конфиденциальной информации в устной форме.

Объектом исследования в данной диссертации выступает ООО «Вектор».

Предметом исследования в выпускной квалификационной работе являются угрозы информационной безопасности со стороны собственного персонала.

Информационная база исследования: учебно-методическая литература, профильные публикации и ресурсы Интернет, внутренние регламенты организации.

Методы исследования: наблюдение, обобщение, сравнительный и статистический анализ.

Методологической и теоретической основой выпускной квалификационной работы явились труды отечественных и зарубежных специалистов в области информационной безопасности.

Практическое использование результатов исследования: повышение информационной безопасности организации в части защиты от угроз по кадровому направлению деятельности.

Структурно выпускная квалификационная работа состоит из введения, основной части, разделенной на три главы и параграфы, заключения и списка использованной литературы.

Глава 1. Нелояльные и безответственные сотрудники как субъекты угроз информационной безопасности работодателя

1.1. Понятие и виды конфиденциальной информации, угрозы репутационным и имущественным интересам организации в случае ее разглашения

Значительное повышение роли информации в жизни личности, общества и государства сделало ее одной из важнейших составляющих жизни общества. В настоящее время в России, как и во всем мире, активно продолжает развиваться информационное общество.

В самом общем виде, можно выделить следующие виды защищаемой информации:

- секретная информация.
- конфиденциальная информация.

Конкретизируя смысловое значение понятия, А.А. Шиверский, подчеркивает, что «тайна, это понятие, имеющее несколько смысловых значений. В целом тайну принято понимать как нечто ещё непознанное. В этом смысле её употребляют в отношении явлений, сущность которых пока не постигнута человеком, то есть тайна как объективная категория, хотя она может быть в любое время познана и в силу этого раскрыта. Как правило, это законы природы или общества»[1].

Тайна может рассматриваться и как субъективная категория. В этом смысле она определяется как сведения, которые какой-либо субъект скрывает от других. Следовательно, понимание тайны как объективной или субъективной категории зависит от того, кто её устанавливает и что является тайной[2].

[1] Шиверский А. А. Защита информации: проблемы теории и практики. М.: Юристъ, 1996. С. 12-13.
[2] Степанов А. Г., Шерстнева О. О. Защита коммерческой тайны. М.: Альфа-Пресс, 2006. С. 34.

Кроме того, трактовка тайны, приведённая из словаря Ожегова И. и Шведовой Н., позволяет заключить, что здесь не идёт речь только об информации. Следовательно, понятие «тайна» может означать что угодно, а не только информацию. Отсюда вытекает, что содержание понятия «тайна» нужно выяснять в каждом конкретном случае.

Если же исходить из того, что нечто скрывается субъектом, как правило, из соображений защиты своих прав и интересов, то тайна выступает в качестве способа их защиты. В этом смысле тайна – есть сокрытие чего-либо.

Резюмируя изложенное, нужно сказать, что «тайна» широкое понятие, которое может означать и объект защиты, и способ защиты объекта. При этом использоваться могут оба понятия. Это позволяет подчеркнуть условность термина «тайна». Конечно, в интересах исключения терминологической путаницы, недопустимо использование в законодательстве понятия «тайна» в двух смысловых значениях. Но автору трудно согласиться с тем, что «тайна» в законодательстве означает вид информации. Это может означать, что, например, в случае сокрытия субъектом иного, чем информация, объекта, тайны нет. Кроме того, следует исходить из назначения института тайны, а именно, из того, что субъект прибегает к сокрытию чего-либо как к мере защиты своих прав и интересов[3].

Институт тайны охватывает достаточно однородные общественные отношения, возникающие в различных сферах деятельности личности, общества, государства. Содержание любой тайны заключается в том, что предмет тайны образует сведения, не предназначенные для широкого круга лиц[4].

Исходя из вышеприведенных определений тайны, одним из основных признаков конфиденциальной информации являются ограничения, вводимые собственником информации на ее распространение и использование.

---

[3] Омарова А. Б. Гражданско-правовые проблемы института коммерческой тайны: дисс… канд. юр. наук. М., 2001. С. 43.

[4] Ярочкин В. И., Шевцова Т. А. Словарь терминов и определений по безопасности и защите информации. (Безопасность предпринимательства). М.: Ось-89, 2008.С. 32.

Информационным процессам присущи определенные закономерности. Наиболее общими являются: постоянный рост количества информации, ее кругооборот, рассеяние и старение информации. Отметим ряд особенностей, которые присущи конфиденциальной информации.

Конфиденциальная информация обладает определенным свойством: если эта информация является основанием для создания новой информации (документов, изделий и т.п.), то созданная на этой основе информация является, как правило, секретной.

Важно подчеркнуть, что появление новой защищаемой информации есть результат деятельности субъекта - собственника информации или уполномоченных им лиц, засекретивших информацию. Она после этого как бы отчуждается от субъекта - автора. Отчуждение защищаемой информации от субъекта, ее создавшего, имеет особенности, состоящие в том, что эта секретная или конфиденциальная информация диктует всем, кто с нею сталкивается, правила обращения с нею, уровень защитных мер к себе и т.д[5]. Соответственно, можно предположить, что уровень защиты информации определяется грифом секретности или конфиденциальности.

Правовая охрана конфиденциальной информации осуществляется на уровне кодифицированных актов, законов и подзаконных нормативно-правовых актов. Рассматривая информацию с ограниченным доступом как вид информации, исходим из того, что такие сведения в полном объеме обладают свойствами информации как субстанции, как социального и правового явления.

Информация с ограниченным доступом в частности включает в себя: информацию, которая охватывает сведения в сфере экономики, обороны, внешних отношений, науки и техники, охраны правопорядка и государственной безопасности, разглашение которых нанесёт (или может нанести) некоторый ущерб национальной безопасности страны. Также к информации с ограниченным доступом относится информация, которая не

[5] Бачило И.Л. Информационное право: основы практической информатики. М.: Вектор,2007. С. 97.

подлежит обнародованию и (или) распространению в средствах массовой информации согласно действующему законодательству.

Информация и данные с ограниченным доступом могут распространяться без согласия их владельца (владельцев), в том случае, если они имеют важное значение для общества - являются предметом общественного интереса и права общественности узнать эту информацию, преобладают над правом владельцев на ее защиту.

Действующие в Российской Федерации нормативно-правовые акты, достаточно скупы в определении дефиниции конфиденциальная информация.

Исходя из этого, конфиденциальную информацию можно определить как ту информацию, в отношении которой ее обладатель установил требование не предоставлять ее третьим лицам без его разрешения. Однако данной формулировки конфиденциальной информации явно недостаточно[6].

Утративший в настоящее время силу Федеральный закон «Об информации, информатизации и защите информации» от 20.02.1995 г. № 24-ФЗ[7] определял конфиденциальную информацию как документированную информацию, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Поскольку в ныне действующей норме указания на признак документированности конфиденциальной информации нет, можно сделать вывод, что информация может носить конфиденциальный характер независимо от ее формы.

Таким образом, конфиденциальная информация, понятие достаточно широкое, отнести к конфиденциальной можно любую информацию, которая, так или иначе, отвечает требованиям ст. 2 Закона об информации.

Можно сделать вывод, что основными видами конфиденциальной информации при классификации по критерию предметного содержания выступают, рисунок 1.

---

[6] Валитова Л. И. К вопросу об ограничении права на информацию // Право и государство: теория и практика. 2011. N 6. С. 32-35.

[7] Об информации, информатизации и защите информации. Федеральный закон от 20.02.1995 г. N 24-ФЗ [Недейств.]

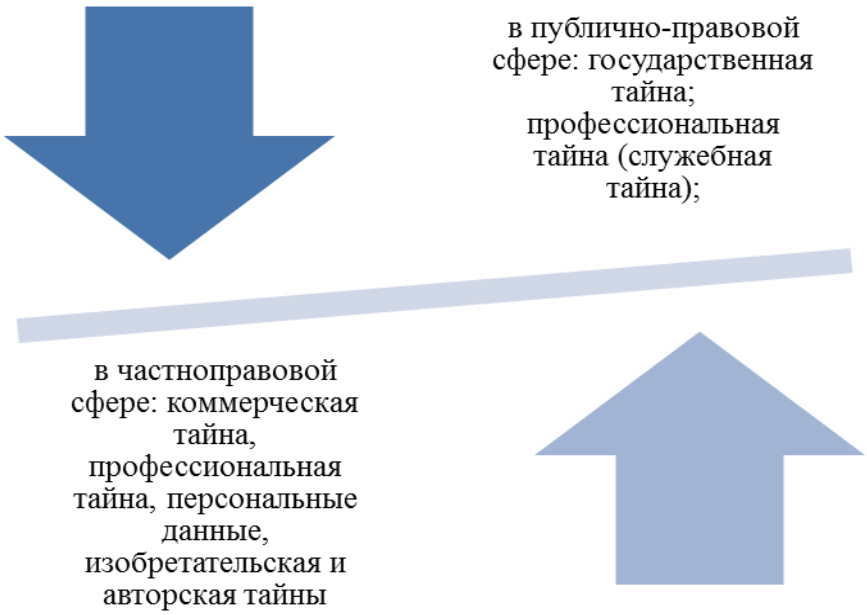


Рисунок 1 - Основные виды конфиденциальной информации при классификации по критерию предметного содержания

Вся информация, которая находится в распоряжении определенных лиц, организаций или органов власти и может подпадать под правовой режим конфиденциальной информации, описывается в современной литературе посредством такой общей разновидности конфиденциальной информации, как служебная тайна. При этом выделяется два вида сведений, которые относятся к служебной тайне органов власти[8]:

- во-первых, это собственная тайна органа власти, представляющая собой оригинальную охраноспособную информацию, выработанную самим органом власти;
- во-вторых, это тайна других лиц, конфиденциальные сведения о гражданах и организациях, собранные органом власти, в процессе реализации установленных для него полномочий.

В целом, вопрос определения конфиденциальной информации — не только теоретический, он имеет и важное практическое значение при реализации административно-правовых режимов конфиденциальной

[8] Щадрин, С. Ф. Уголовно-правовая охрана служебной тайны: Автореф… дисс… канд. юр. наук. Ростов-на-Дону,2002. С. 12-13.

информации, а именно при привлечении лица к ответственности за распространение сведений, носящих конфиденциальный характер.

Не меньше практических сложностей возникает при определении того, что понимать под разглашением конфиденциальной информации[9]. Так, например, дискуссионным является вопрос о том, считать ли разглашением просто пересказ содержания документа или разглашением будет являться опубликование или передача третьим лицам самого документа или его копию[10].

Закон об информации не указывает, какие действия можно трактовать как распространение информации. Если обратиться к Федеральному закону «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ3 (далее — Закон о коммерческой тайне), то из его текста следует, что разглашение есть действия, в результате которых информация становится известной третьим лицам в любой возможной форме, как устной, так и письменной (п. 9 ст. 3).

Тем самым, обязанность не разглашать конфиденциальную информацию можно определить как запрет на ее предоставление, т. е. передачу определенному кругу лиц (п. 8 ст. 2 Закона об информации), а также на распространение, т. е. передачу неопределенному кругу лиц (п. 9 ст. 2 Закона об информации).

Для целей исследования, также считаем необходимым остановиться на определениях основных видов конфиденциальной информации. К таковым относятся:

1) «Государственная тайна – вид информации, на которую распространяется самый жесткий режим ограничения доступа. В настоящее время помимо государственной тайны выделяют множество институтов конфиденциальной информации, многие из которых пересекаются либо дублируют друг друга.

[9] Башаратьян М. К. Система конституционных прав и свобод граждан Российской Федерации в сфере деятельности средств массовой информации: дисс. ... канд. юрид. наук. М., 2007. С. 79-80.
[10] Кучеренко А. В. Информация как объект правового регулирования // Вестник Амурского государственного университета. 2007. N 36. С. 39.

Так, различными исследователями выделяются служебная, коммерческая, профессиональная, военная, банковская, страховая, личная и семейная, адвокатская и другие виды тайн. Указанные виды конфиденциальной информации нельзя строго отграничить друг от друга, поскольку многие из перечисленных понятий взаимосвязаны и частично дублируют друг друга. Однако предпринимаются попытки систематизации групп конфиденциальной информации, на рассмотрении которых остановился автор ниже.

В настоящее время, секретные сведения отнесены к государственной тайне, однако понятие служебной тайны наличествует в некоторых нормативно-правовых актах.

2) Профессиональная тайна. Данное понятие является самым широким ввиду большего круга субъектов. Традиционно к профессиональной тайне относится не являющаяся общедоступной информация, полученная конфидентом в ходе осуществления профессиональной деятельности (врачебная, нотариальная, адвокатская и иные виды тайн).

Существует мнение, с которым, вероятно, следует согласиться, об отнесении к разряду профессиональной тайны банковской, налоговой тайны, тайны страхования, усыновления, исповеди, предварительного следствия. Отнесение тайны предварительного следствия к разряду профессиональной весьма условно. Отнесение запрета на разглашение информации о предварительном следствии, предусмотренного ст. 310 УК РФ[11] к профессиональной тайне не представляется возможным ввиду несоответствующего этому виду тайны конфидента. Возможно отнесение к профессиональной тайне сведений о частной жизни, ставших известными органу предварительного расследования и не относящихся к предмету доказывания по делу (не относящихся к предмету расследования).

[11] Уголовный кодекс Российской Федерации. Федеральный закон от 13.06.1996 N 63-ФЗ (ред. от 19.04.2013)

Отнесение налоговой тайны к профессиональной возможно, однако следует отметить, что налоговая тайна с некоторыми допущениями является и служебной. Режим налоговой тайны установлен ст. 102 Налогового кодекса РФ[12], а также иными законами и подзаконными актами. Налоговая тайна не во всех случаях является профессиональной. Так, по смыслу ст. 183 УК РФ налоговая тайна может не только быть получена в ходе профессиональной деятельности, но и быть доверена лицу. Таким образом, не во всех случаях налоговая тайна может быть отнесена к профессиональной.

К профессиональной тайне относится и банковская тайна. При этом исследователи[13] отмечают несоответствия между нормами ГК РФ и Федерального закона «О банках и банковской деятельности»[14]. В Федеральном законе «О банках…» понятие банковской тайны более широкое, нежели в ГК РФ. Так, Федеральный закон «О банках…» в ст. 26 устанавливает обязанность по неразглашению кредитными организациями информации об операциях, вкладах, счетах, тогда как в ст. 857 ГК РФ речь идет об обязанности банка не разглашать информацию об операциях по счету и информации о клиенте.

Таким образом, исходя из особенностей профессиональной деятельности, законодательство устанавливает гарантии соблюдения профессиональной тайны, а ответственность предусмотрена для первичных видов тайн.

В целом, в настоящее время насчитывается порядка шестидесяти видов конфиденциальной информации, что, в свою очередь, ведет к необходимости определенной классификации конфиденциальной информации.

Классификация информации по степени ее секретности (конфиденциальности) без отнесения ее к какому-то конкретному виду

[12] Налоговый кодекс Российской Федерации. Часть первая. Федеральный закон от 31.07.1998 N 146-ФЗ (ред. от 04.04.2013)
[13] Семашко А.В. Правовые основы оборота информации с ограниченным доступом (конфиденциальной информации) в Российской Федерации: Автореф… дисс… канд. юр. наук. М., 2008. С. 17.
[14] О банках и банковской деятельности. Закон РФ от 02.12.1990 N 395-1 (ред. от 26.03.2013)

выглядит несколько абстрактной. Но она дает представление о возможности ранжирования защищаемой информации по степени ее важности для собственника.

По содержанию защищаемая информация может быть - политической, экономической, военной, разведывательной и контрразведывательной, научно-технической, технологической, деловой и коммерческой.

Информация может быть рассмотрена с точки зрения отображения ее на каких-то или в каких-то материальных (физических) объектах, которые длительное время могут сохранять ее в относительно неизменном виде или переносить ее из одного места в другое.

В научной литературе можно найти несколько попыток классификации конфиденциальной информации, ни одна из которых не получила достаточно широкого признания, что тоже свидетельствует об актуальности данной проблемы[15].

Например, А. А. Фатьянов[16] классифицирует подлежащую защите информацию по трем признакам: по принадлежности, по степени конфиденциальности (степени ограничения доступа) и по содержанию. Существуют и другие классификации[17].

Вместе с тем при этих подходах выпадает такой существенный признак конфиденциальной информации, как причина возникновения или обладания ею как владельца, так и пользователя. Хотя такой признак намного облегчил бы установку норм, регулирующих порядок работы и защиты конфиденциальной информации в зависимости от причин ее возникновения. Ведь человек как субъект информации может по-разному отнестись к своей персональной и конфиденциальной информации, которая оказалась известна ему в силу его служебного положения или профессиональных обязанностей.

---

[15] Алексенцев А. И О классификации конфиденциальной информации по видам тайны // Безопасность информационных технологий. 1999. N 3. С. 48-53.

[16] Фатьянов А. А. Концептуальные основы обеспечения безопасности на современном этапе // Безопасность информационных технологий. 1999. N 1. С. 26-40.

[17] Тиновицкая И. Д. Правовая информация: законодательные проблемы // Проблемы информатизации. 2005. N 1.; Ефремов А. А. Понятие и виды конфиденциальной информации // Право и экономика. 2004. N 4: и др.

1.2.Основные угрозы информационной безопасности организации, исходящие от ее безответственных и нелояльных сотрудников

Конфиденциальность, целостность и доступность информации могут существенно способствовать обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации. Зависимость от информационных систем и услуг означает, что организации становятся все более уязвимыми по отношению к угрозам безопасности, которые могут быть определены как совокупность действий, направленных на нарушение одного из трех свойств информации – *конфиденциальности*, *целостности* или *доступности*.

Источники угрозы информационной безопасности организации - это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности, рисунок 2.

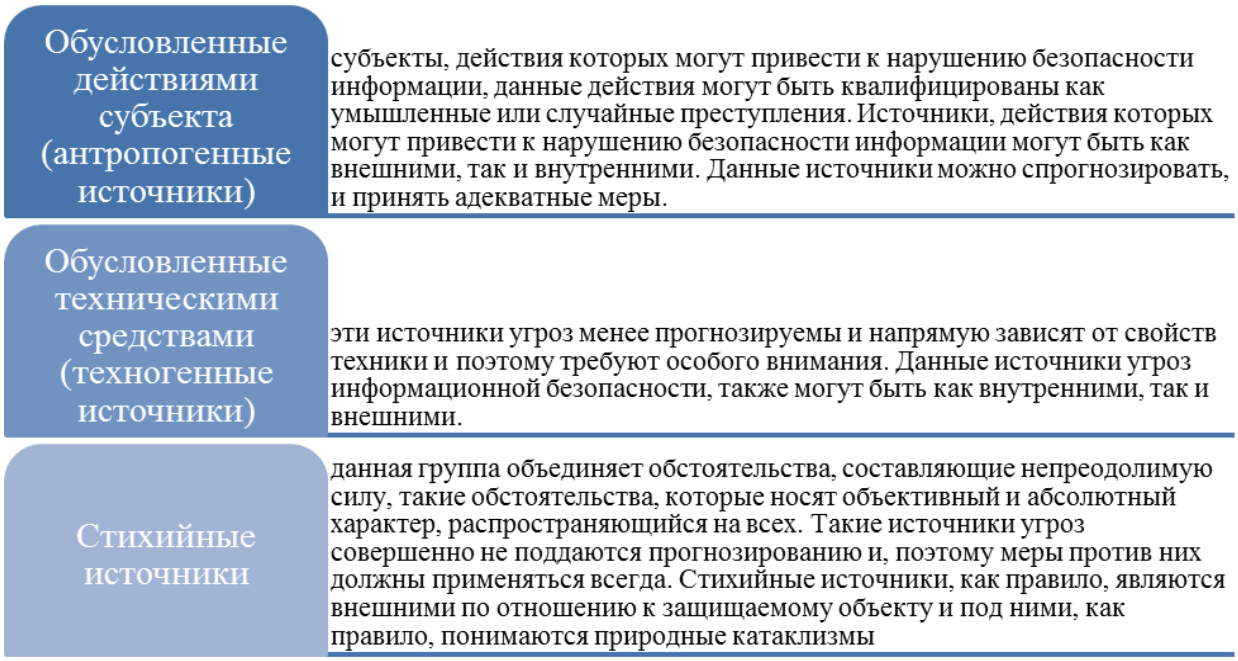


Рисунок 2 - Источники угрозы информационной безопасности организации[18]

[18] Девянин П.Н. Садердинов А.А., Трайнев В.А. и др. «Информационная безопасность предприятия» Учебное пособие, - М., 2006.

Угрозы информационной безопасности организации делятся на два основных типа – это естественные и искусственные угрозы, рисунок 3.

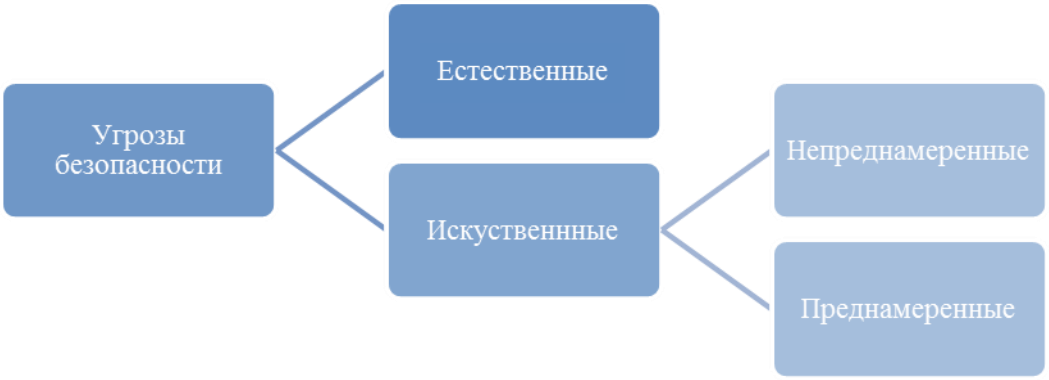


Рисунок 3- Классификация угроз информационной безопасности организации

К естественным угрозам информационной безопасности организации относятся пожары, наводнения, удары молний и другие стихийные бедствия и явления, приводящие к аварийным ситуациям, возникновение которых не зависит от человека.

Для обеспечения безопасности информации в организации, необходимым условием является оборудование помещений, в которых находятся элементы системы (носители цифровых данных, серверы, архивы и пр.).

Искусственные угрозы информационной безопасности организации – это угрозы, вызванные деятельностью человека. Они могут быть преднамеренными и непреднамеренными, (т.е. случайными). Система должна быть устойчива как к случайным, так и к преднамеренным враждебным воздействиям.

Угрозы, носящие случайный характер, или непреднамеренные угрозы, связаны с отказами, сбоями аппаратуры, ошибками операторов и т.п. Фактор появления таких угроз обусловлен ограниченной надежностью работы человека и техники.

Угрозы, носящие злоумышленный характер, или преднамеренные угрозы информационной безопасности организации, вызваны, как правило,

преднамеренным желанием субъекта осуществить несанкционированные изменения с целью нарушения корректного выполнения преобразований, конфиденциальности, достоверности и целостности данных.

Данный класс угроз очень динамичен и постоянно пополняется.

К умышленным угрозам информационной безопасности организации относятся:

- несанкционированный доступ к конфиденциальной информации и сетевым ресурсам;
- раскрытие и модификация данных и программ, их копирование;
- раскрытие, модификация или подмена трафика вычислительной сети;
- разработка и распространение компьютерных вирусов, ввод в программное обеспечение логических бомб;
- кража магнитных носителей и расчетных документов;
- разрушение архивной информации или умышленное ее уничтожение;
- фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;
- перехват и ознакомление с информацией, передаваемой по каналам связи, и т. п.

По расположению источника, угрозы делятся на внутренние и внешние.

Внешние угрозы исходят от конкурентов, стремящиеся нанести ущерб деятельности организации. Например, мотивационная система сотрудников у конкурирующей организации лучше, чем у компании и это станет определяющим фактором при переходе сотрудника к конкурентам[19]. В данном случае тот факт, что у конкурентов лучше проработана система мотивационной составляющей не являлась угрозой, но при сравнении двух компании стала решающим перевесом. Так же к внешним угрозам относится

[19]Рэдхед К. Управление финансовыми рисками на стратегическом уровне М: ИНФРА-М – 2013- с.125

давление на сотрудников извне, попадание сотрудников в различные виды зависимостей, инфляционные процессы[20].

К внутренним угрозам отрицательным факторам влияния относится несоответствие квалификации работника предъявляемым требованиям компании, слабая система по обучению работников, некачественная первичная проверка соискателей в кандидаты, неграмотная социальная и корпоративная политика организации в целом, отсутствие стратегии развития и совершенствования кадровой системы, в том числе и кадровой безопасности. Эти вещи наносят любой компании в той или иной степени не только имиджевый ущерб, но и экономический только имиджевый ущерб, но и экономический.

В общем случае выделяют три основных вида умышленных угроз безопасности: угрозы конфиденциальности, целостности и доступности.

Свойство конфиденциальности информации позволяет не давать права на ее доступ или не раскрывать ее неполномочным лицам, логическим объектам или процессам.

Нарушение конфиденциальности информации, это, прежде всего, ее кража или перехват и расшифровка сетевых пакетов, т.е. анализ трафика. Обычно с реализацией этой угрозы и начинается большинство серьезных атак. Угроза нарушения целостности включает в себя любое умышленное изменение (модификацию или удаление) данных, хранящихся в системе. Доступность информации – это свойство информации быть доступной и используемой по запросу со стороны любого уполномоченного пользователя. Угроза отказа в обслуживании возникает каждый раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы.

Виды угроз случайного и преднамеренного характера приведены в таблице 1. На рисунке 2 представлены программные угрозы информационной безопасности организации.

[20] Сычев Ю. Н. Управление безопасностью и безопасность бизнеса: учебное пособие, 2005- с.12.

Таблица 1

Виды угроз информационной безопасности организации случайного и преднамеренного характера

Несанкционированные действия	
Случайные	**Преднамеренные**
● Ошибки в программном обеспечении ● Ошибки в работе персонала ● Отказы и сбои оборудования ● Помехи в линиях связи из-за воздействий внешней среды ● Несанкционированный доступ: случайное ознакомление с конфиденциальной информацией посторонних лиц	● Нарушение конфиденциальности информации (кража данных, перехват и расшифровка сетевых пакетов) ● Нарушение целостности информации (модификация или удаление данных) ●Нарушение доступности информации (отказ в обслуживании) Методы воздействия: ● Вредоносные программы (вирусы, черви, троянские программы, программы-шпионы и др.). ● Программы, организующие DoS-атаки и другие атаки, спам, несанкционированный доступ (перехват и взлом паролей, взлом ОС, взлом приложений и протоколов (TCP/FTP/SSH/DNS/HTTP/SMTP/ протоколов маршрутизации)

В соответствие с методикой определения актуальных угроз безопасности рассмотрим следующие угрозы (таблица 1).

Вероятность возникновения угроз информационной безопасности могут быть: маловероятные угрозы, низко-вероятностные угрозы, средне-вероятные угрозы и высоко-вероятностные угрозы.

При оценке опасности определяется вербальный показатель опасности: низкая опасность, средняя опасность и высокая опасность.

Таблица 2

Выявление актуальных угроз информационной безопасности организации

Угроза безопасности	**Вероятность возникновения**	**Опасность**	**Актуальность**
Внутренние источники угрозы безопасности			
Антропогенные источники			
Разглашение защищаемой информации лицами, имеющими к ней право доступа	Средняя	Высокая	актуальная
Неправомерные действия со стороны лиц, имеющих право доступа к информации	Высокая	Высокая	актуальная
Несанкционированный	Высокая	Высокая	актуальная

доступ к информации			
Ошибки обслуживающего персонала	Низкая	Средняя	неактуальная
Техногенные источники			
Дефекты, сбои и отказы программного обеспечения	Низкая	Высокая	актуальная
Дефекты сбои и отказы технических средств	Низкая	Высокая	актуальная
Наводка	Низкая	Средняя	неактуальная
Паразитное электромагнитное излучение	Низкая	Низкая	неактуальная
Излучение сигналов	Низкая	Низкая	неактуальная
Внешние источники угрозы безопасности			
Антропогенные источники			
Доступ к защищаемой информации с применением технических средств	Низкая	Высокая	актуальная
Действия криминальных групп	Низкая	Средняя	неактуальная
Искажение, уничтожение или блокирование информации с применение технических средств	средняя	Высокая	актуальная
Угроза безопасности	**Вероятность возникновения**	**Опасность**	**Актуальность**
Техногенные источники			
Явления техногенного характера	Низкая	низкая	неактуальная
Стихийные источники			
Стихийные бедствия, природные явления	Низкая	низкая	неактуальная

1.3.Основные методы защиты конфиденциальной информации от угроз со стороны собственного персонала организации

Каждое предприятие оснащено компьютерной техникой и доступом к всемирной паутине Интернет. Злоумышленники умело подключаются практически к каждой составной этой системы и с помощью многочисленного арсенала (вирусы, вредоносное ПО, подбор паролей и другое) воруют ценную информацию. Система информационной безопасности должна внедряться в каждую организацию. Руководителям

необходимо собрать, проанализировать и классифицировать все виды информации, которая нуждается в защите, и использовать надлежащую систему обеспечения безопасности. Но и этого будет мало, потому что, кроме техники, существует еще и человеческий фактор.

Важно правильно организовать защиту своего предприятия на всех уровнях. Для этих целей используется система менеджмента информационной безопасности, с помощью которой руководитель наладит непрерывный процесс мониторинга бизнеса и обеспечит высокий уровень безопасности своих данных.

Но, к сожалению, далеко не все руководители считают необходимым защищать свои предприятия, мотивируя свое решение отсутствием важной информации в своем бизнесе. Это неправильно.

Подходы к выстраиванию комплексной системы информационной безопасности критически важных предприятий, нуждающихся в обеспечении целостности, доступности и конфиденциальности информации, имеющих свои особенности и специфику, которые должны быть учтены еще на этапе построения концепции защиты.

Попробуем рассмотреть основные моменты снижения рисков и борьбы с угрозами в инфраструктуре промышленных предприятий. Обеспечение комплексной безопасности инфраструктуры промышленного предприятия имеет свою специфику.

Упрощенная схема взаимосвязей в рамках функционирования промышленной системы приведена на рисунке 4.

Если автор имеет дело с десятками промышленных цехов, распределенных на территории в несколько десятков квадратных километров, то для доступа к корпоративным ресурсам могут потребоваться беспроводные точки подключения (Wi-Fi), которые также нужно контролировать. Если разнородные централизованные информационные системы концентрируются в едином дата-центре, через который идут все

потоки информации, то может потребоваться реализация единой системы управления учетными данными пользователей (системы класса IDM).

Рисунок 4 - Упрощенная схема взаимосвязей в рамках функционирования системы

Если же речь идет об обеспечении безопасного мобильного доступа к информационным ресурсам предприятия, то для этого могут быть использованы распространенные сейчас MDM-системы, позволяющие управлять мобильными устройствами.

Например, несколько лет назад специалисты компании КРОК помогли ОАО “Авиадвигатель”, где работают более 2 500 человек, обеспечить для сотрудников доступ к основным корпоративным приложениям с их собственных мобильных устройств. Было внедрено комплексное решение, состоящее из MDM-системы и подсистемы SSL VPN для защищенного доступа к внутренним ИТ-ресурсам предприятия.

Но в целом, комплексный подход к защите информации на промышленном предприятии примерно тот же, что и на любом другом территориально распределенном предприятии. В отличие от банков или сотовых операторов, где отраслевые требования к информационной безопасности задаются внешним регулятором, в промышленности их определяет собственник холдинга или совет директоров, который может

определить ту или иную парадигму защиты, четко учитывающую основные риски и угрозы.

Процесс разглашение конфиденциальной информации – несанкционированное доведение защищаемой информации до лиц, которые не имеют права доступа к этой информации.

Информационная безопасность - это защищенность информации от незаконного ознакомления в первую очередь, а также преобразования и уничтожения. Природа воздействий, которые направлены на нарушение безопасности может быть самой разнообразной.

В данном разделе рассмотрены факторы, способствующие разглашению защищаемой информации лицами, имеющими к ней право доступа и методы для предупреждения и борьбы с ними:

- Ответственность за разглашение (подписка о неразглашении).
- Контрольно-пропускной режим.

Это комплекс организационно-правовых ограничений и правил, которые устанавливают порядок пропуска через контрольно-пропускные пункты в отдельные помещения сотрудников объекта, посетителей, транспорта и материальных средств. Контрольно-пропускной режим – это один из ключевых моментов в организации системы безопасности на предприятии.

Контрольно-пропускной режим вводится для того, чтобы исключить:

- проникновение посторонних лиц на охраняемые (режимные) объекты, в административные здания, а также в режимные помещения;
- посещение режимных помещений без служебной необходимости должностными лицами организации;
- внос (ввоз) в административные здания и на объекты личных визуальных средств наблюдения, кино-, видео- и фотоаппаратуры, радиотехнической и другой аппаратуры;
- контроль за использованием мобильного телефона;

На территории предприятия нельзя пользоваться незарегистрированным мобильным телефоном. Если же телефон зарегистрирован, то нельзя пользоваться фото-видео съемками, выходом в Интернет.

- вынос (вывоз) из административных зданий и объектов документов и вещей без соответствующего разрешения[21].
- Контроль за подключением к Интернету.

Доступом в Интернет обладает отдельно стоящий компьютер, который не работает в локальной сети.

- Запрет на использование незарегистрированных носителей.

Сегодня, действующие нормативные правовые акты не предусматривают эффективную защиту конфиденциальной информации предприятия, а, следовательно, только комплекс мер (контрольно-пропускной режим, запрет на использование зарегистрированных носителей, подписка о неразглашении) способен обеспечить полноценную защиту организации от разглашения и снизить риск возникновения подобной ситуации.

Неправомерные действия со стороны лиц, имеющих доступ к информации

Для того чтобы защититься от неправомерных действий со стороны лиц, имеющих право доступа к информации, рассмотрим типичные ошибки, которые допускает руководство на промышленных предприятиях.

Исходя из вышеперечисленного, можно сделать вывод, что необходимо внедрять целый комплекс методов и средств защиты от неправомерных действий со стороны лиц, имеющих право доступа к информации, так как вероятность каждой отдельной угрозы очень велика, а исключить все сразу можно лишь используя весь комплекс методов и средств, а именно:

[21] Соколов А.В., Степанюк О.М. «Защита от компьютерного терроризма» Справочное пособие. - СПб.: БХВ - Петербург, Арлит, 2002

1. Контрольно-пропускной режим.

2. Ведение журналов регистрации действий пользователей.

Необходимо осуществлять контроль за действиями пользователей. Собирать и хранить информацию обо всех событиях, которые происходят в системе.

3. Осуществление резервного копирования.

Резервным копированием является процесс создания копии данных на носителе (жёстком диске, дискете и т.д.), которое предназначено для восстановления данных в оригинальном или новом месте их расположения в случае их разрушения или повреждения.

Для того, чтобы защититься от несанкционированного доступа к информации необходимо использовать алгоритмы защиты информации (прежде всего шифрования). Их можно реализовать как программными, так и аппаратными средствами.

Таблица 3

Сравнительный анализ средств шифрования

Критерии оценки	Аппаратные средства	Программные средства
Стоимость покупки и эксплуатации за 1 шт. за 1 год	~2500 руб.	~1800 руб.
Возможность реализовать систему разграничения доступа к компьютеру	+	+
Скорость шифрования	до 80 МБ/с	до 60 МБ/с
Дополнительная нагрузка на центральный процессор компьютера	-	+
Защита от вредоносных программ	+	+
Наличие систем идентификации и аутентификации	+	+

Согласно сравнительному анализу средств шифрования, представленному в Таблице 3, видно, что для производства целесообразнее использовать аппаратный вариант защиты от несанкционированного доступа к информации.

Аппаратный шифратор представляет собой компьютерное «железо», чаще всего это плата расширения, вставляемая в разъем ISA или PCI системной платы ПК, или USB-ключ с криптографическими функциями.

Рассмотрим подробнее методы работы шифратора для защиты от несанкционированного доступа:

- Распределение прав доступа.

При распределении прав доступа выясняются функции, которые должны исполнять те или иные группы пользователей. Исходя из этого, определяются данные, к которым пользователи различных групп будут иметь доступ.

- Защита от вредоносных программ.
- Системы идентификации и аутентификации.

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем является идентификацией. Процесс идентификации обеспечивает выполнение следующих функций:

- установка подлинности и определение полномочий субъекта при его допуске в систему;
- контролироль установленных полномочий в процессе сеанса работы;
- регистрация действий и др.

На современном этапе состояния общества информационные технологии активно внедряются во все сферы национальной экономики. Сегодня руководство любого промышленного предприятия, по существу, имеет дело с корпоративной информацией, на основе которой принимаются ответственные решения. Такая информация должна соответствовать требованиям актуальности, достоверности, структурированности и 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.

Для защиты информации от актуальных угроз, на основании сравнительного анализа, были выбраны методы и средства защиты. Кроме того, во время проведения обучения пользователей во избежание возникновения непреднамеренных угроз безопасности им должны быть разъяснены их обязанности и возможности системы.

В целом можно отметить, что информационная безопасность должна стать важнейшей частью корпоративной культуры компании, подкрепленной комплексом программно-технических и организационных мер, которые позволят минимизировать риски подобного рода.

Краткие выводы по главе

В ходе выполнения первой главы, которая была посвящена теоретическим основам угроз информационной безопасности работодателя, автор пришел к следующим выводам:

1. Целью информационной безопасности является безопасность информационных ресурсов в любой момент времени и в любой обстановке.

2. Одним из существенных проявлений несовершенства информационного законодательства является отсутствие четких законодательных критериев для определения конфиденциальной информации, порядка и условий отнесения информации к конфиденциальной. Такие пробелы затрудняют реализацию прав на информацию.

3. Информационная безопасность должна стать важнейшей частью корпоративной культуры компании, подкрепленной комплексом программно-технических и организационных мер, которые позволят минимизировать риски подобного рода.

4. Руководству предприятия необходимо самому позаботиться о

секретах компании. Действующие нормативные правовые акты не предусматривают эффективную защиту конфиденциальной информации организации.

Глава 2. Практика противодействия угрозам информационной безопасности организации ООО «Вектор» со стороны собственного персонала

2.1. Краткая характеристика организации и анализ динамики ее кадрового потенциала за 2017-2019 гг.

Основной сферой деятельности компании является продажа новых иномарок. Вектор представляет 21 автомобильную марку – Nissan, Volkswagen, Renault, Opel, Infiniti, Chevrolet, KIA, Hyundai, Mazda, Škoda, Toyota, Ford, Cadillac, Suzuki, Citroën, Datsun, Mitsubishi, SsangYong, Peugeot, Lada и УАЗ[22].

Компания объединяет 48 дилерских центров: 19 в Москве, 26 – в регионах (Санкт-Петербург, Брянск, Воронеж, Самара, Ярославль, Челябинск, Екатеринбург, Новосибирск, Архангельск, Сургут, Новокузнецк, Саратов и Краснодар) и 3 – в Казахстане (Астана, Алматы, Караганда). По итогам 2015 года доля федерального рынка компании «Вектор» составила 2,9%, доля столичного рынка – 6,5%. В штате компании более 6 000 сотрудников[23].

В 2016 году, по собственному сообщению, «Вектор» продал 52 079 автомобилей (41 046 новых и 11 033 с пробегом). В 2016 году выручка составила 60,3 млрд. рублей (в 2005 году — $772,2млн.), ожидаемая по итогам года чистая прибыль — $13 млн. Группа компаний «Вектор» (ГК «Вектор») – крупнейший розничный автомобильный дилер на российском рынке. По итогам 2016г. доля федерального рынка Компании в сегменте новых легковых автомобилей составила 2,4%, доля столичного рынка – 4,8%[24].

Группа компаний «Вектор» была основана в 1993 году и за время своей

22 Официальный сайт ГК «Вектор» [электронный ресурс]: http://www.vektorauto/
23 По данным внутренней отчетности ГК «Вектор» - не опубликовано
24 По данным внутренней отчетности ГК «Вектор» - [электронный ресурс]: https://www.autostat.ru/news/25500/

активной деятельности стала одним из самых крупных официальных автодилеров России. В салонах ГК «Вектор» представлены в наличии автомобили более 18 известных марок, полный список которых был упомянут выше. На территории России ГК «Вектор» представлена широкой сетью дилерских центров, расположенных в Москве, Санкт-Петербурге, Екатеринбурге, Краснодаре, Воронеже и т. д. Кроме того, представительства есть в Республике Казахстан (в Астане, Алма-Аты и Караганде).

Таким образом, предприятие ГК «Вектор» является активно развивающимся предприятием, с разветвленной филиальной сетью. Такое построение бизнеса требует организации системы информационного обеспечения, защищенного от возможных рисков, в том числе и со стороны злоупотребления персоналом.

Объектом исследования выступает подразделение ГК «Вектор», курирующего работу с марками автомобиля «Хендай» - ООО «Вектор-Трейд», зарегистрированного по адресу: Российская Федерация, 107497, г. Москва, ул. Иркутская, д. 5/6, стр. 1, помещение 321.

К основным направлениям работы подразделения относится обеспечение взаимодействия между структурными подразделениями организации, поставщиками и контрагентами, контроль и обеспечение работы дилерских центров и станций ТО. А также непосредственное управление тремя специализированными салонами:

1. ДЦ Вектор - Сокольники (Москва) Адрес: г. Москва, ул. Краснобогатырская, дом 2, строение 26;
2. ДЦ Вектор - Марьино (Москва) Адрес: г. Москва, ул. Перерва, дом 19;
3. ДЦ Вектор - Петровско-Разумовская (Москва) Адрес: г.Москва, Дмитровское шоссе, дом 98, стр. 1.

Организационная структура представлена на рисунке 5.

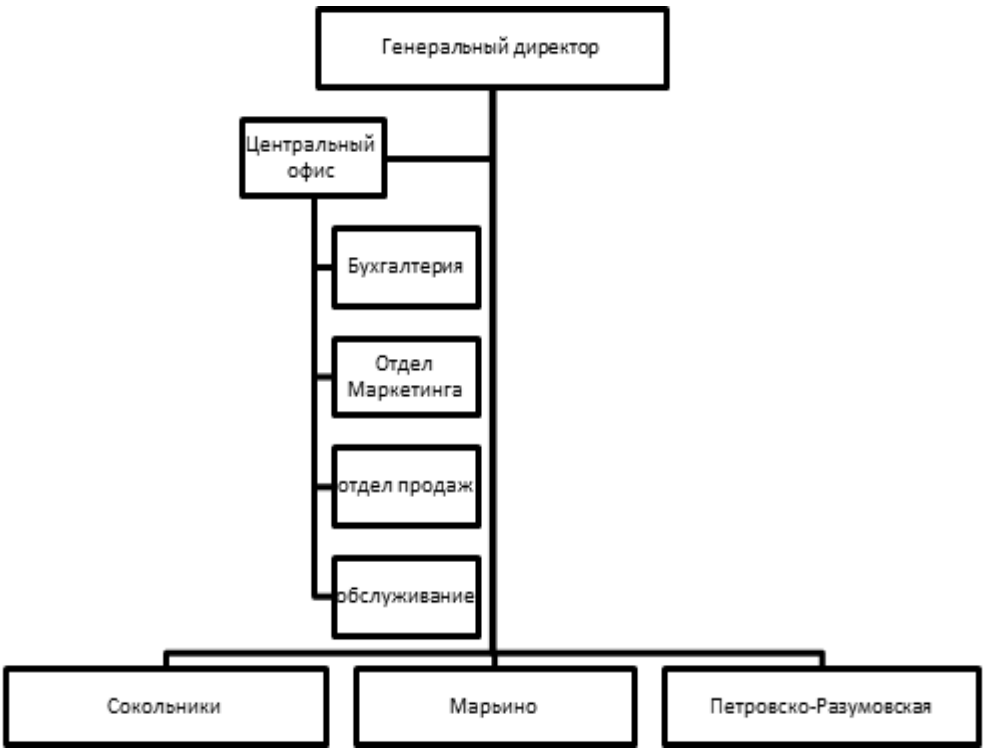


Рисунок 5 - Организационная структура подразделения ГК «Вектор» - Хендай (ООО «Вектор-Трейд)

Основные задачи анализа:

– изучение обеспеченности организации и его структурных подразделений персоналом по количественным и качественным параметрам;

– оценка экстенсивности, интенсивности и эффективности использования персонала на предприятии;

– выявление резервов более полного и эффективного использования персонала на предприятии.

Источники информации – план по труду, статистическая отчетность «Отчет по труду», данные табельного учета и отдела кадров.

Обеспеченность организации трудовыми ресурсами определяется путем сравнения фактического количества работников по категориям и профессиям с плановой потребностью (Таблица 3).

По данным таблицы 4 можно сделать вывод о том, что в 2018г. произошло увеличение общей численности персонала подразделения «Хендай» на 20,32%. Это свидетельствует об относительном расширении деятельности ГК подразделения, что подтверждается открытием нового

сервисного пункта.

Таблица 4

Обеспеченность ГК «Вектор»- «Хендай» (ООО «Вектор-Трейд») трудовыми ресурсами в 2017-2019г.

Категория работников	Численность работников, чел.			Абс. откл. (2019/2017)	Отн. откл. (2019/2017),%
	2017	2018	2019		
Среднесписочная численность персонала	205	251	302	51	20,32
в том числе:					
управленческий состав	41	53	76	23	43,40
Рядовые сотрудники	164	198	226	28	14,14

При этом численность рядовых сотрудников выросла только на 14,14%, а управленческого персонала – на 43,4%.

Уровень централизации довольно высок, т. к. все важнейшие решения принимаются высшим звеном управления. Обеспеченность трудовыми ресурсами отдельных подразделений ГК «Вектор»-»Хендай» (ООО «Вектор-Трейд») представлена в таблице 4.

Согласно данным таблицы 5, можно сделать следующие выводы относительно персонала подразделений «Хендай» в ГК «Вектор».

Таблица 5

Обеспеченность трудовыми ресурсами отдельных подразделений ГК «Вектор»-»Хендай» в 2017-2019г.

Категория работников	Численность работников, чел.			Абс.откл. (2019/2017), %	Отн.откл. (2019/2017), %
	2017	2018	2019		
Среднесписочная численность персонал, чел.	205	251	302	51	20,32
в том числе:					
Центральный офис	54	63	62	-1	-1,59
- руководители	10	14	17	3	21,43
- специалисты и служащие	21	25	24	-1	-4,00
- Вспомогательный персонал	23	24	21	-3	-12,50
Вектор ДЦ - Сокольники, в том числе:	62	73	68	-5	-6,85
- руководители	11	12	13	1	8,33

- специалисты и служащие	20	21	23	2	9,52
- работники сервисного центра	31	40	32	-8	-20
Вектор ДЦ - Марьино, в том числе:	46	52	51	-1	-1,92
- руководители	10	11	12	1	9,09
- специалисты и служащие	17	18	21	3	16,67
- работники сервисного центра	19	23	18	-5	-21,74
Вектор ДЦ - Петровско-Разумовская, в том числе:	43	63	62	-1	-1,59
- руководители	10	16	16	-	-
- специалисты и служащие	15	19	24	5	26,32
- работники сервисного центра	18	28	22	-6	-21,43

Анализируя структуру подразделений «Хендай» в ГК «Вектор» можно порекомендовать сузить масштаб управляемости, т. е. назначить заместителей начальников отделов. Это позволит снизить количество человек в непосредственном подчинении у начальника отдела.

Для наиболее полного анализа кадрового состава компании ГК «Артомир»-»Хендай» (ООО «Вектор-Трейд») проиллюстрируем динамику изменения количественного состава работников в преломлении основных специальностей и отделов. Необходимо оговориться, что в каждом подразделении ГК «Вектор» существуют аналогичные профессии и отделы, т.е. структура кадрового состава подразделений компании идентична (Таблица 6).

Таблица 6

Распределение персонала Подразделение «Хендай» в ГК «Вектор» по основным структурным подразделениям и отделам в 2017-2019г.

Персонал ГК «Вектор» «Хендай»	**Численность работников, чел.**			**Абс. откл. (2019/2017)**	**Отн. откл. (2019/2017),%**
	2017	2018	2019		
Среднесписочная численность персонала + руководители	205	251	302	51	20,32
в том числе:					
- отдел продаж	59	77	89	12	15,58
- отдел маркетинга	18	20	26	6	30,00

- отдел логистики	15	16	17	1	6,25
- кредитный отдел	11	20	19	-1	-5,00
- экономический отдел и бухгалтерия	25	27	32	5	18,52
- юридический отдел и отдел заключения договоров	17	25	27	2	8,00
- ремонтный цех	37	40	54	14	35,00
- кузовной цех	23	26	38	12	46,15

В ООО «Вектор» отдел логистики совмещает в себе двустороннюю функцию: во-первых, контролирует поставки автомобилей и автозапчастей, а, во-вторых, занимается вопросами таможенного оформления ввиду совмещения функций отдела сбыта.

Увеличение численности отдела продаж ООО «Вектор» на 15,58% в 2019г. по сравнению с 2018г. связано, в первую очередь, с планированием открытия новых дилерских центров «Хендай».

Одним из наиболее важных моментов при анализе кадрового состава организации является разделение персонала по представленным в компании социально-значимым профессиям (Таблица 7).

Таблица 7

Распределение персонала Подразделение «Хендай» в ГК «Вектор» по основным структурным подразделениям и отделам в 2017-2019г.

Персонал ГК «Вектор»-«Хендай»	**Численность работников, чел.**			**Абс. откл. (2019/2017), %**	**Отн. откл. (2019/2017), %**
	2017	2018	2019		
Среднесписочная численность персонала + руководители	205	251	302	51	20,32
в том числе:					
- менеджеры	21	24	32	8	33,33
- экономисты	62	84	75	-9	-10,71
- бухгалтера	6	8	10	2	25,00
- логисты и специалисты по	15	16	17	1	6,25

таможенному оформлению					
- механики	21	24	30	6	25
- механики кузовного цеха	23	26	38	12	46,15
- автослесаря	16	16	24	8	50
- юристы	17	20	24	4	20
- финансисты	24	33	55	22	66,67

Ввиду специфики деятельности ООО «Вектор»-»Хендай» – торговля и оказание дилерских услуг и сервисного обслуживания, основную часть персонала компании составляют работники с экономическим образованием (более 50% от общего числа работников организации) и их доля в профессиональной структуре подразделения «Хендай» в ГК «Вектор» постоянно растет.

В процессе анализа изучаются изменения в составе рабочих по этим признакам, а также их половозрастная структура - представлены в Приложении 1.

Анализ по трудовому стажу проводится в зависимости от стажа работы по конкретной профессии, а не на заданном предприятии, ввиду того, что данная компания еще 7 лет назад не работала на рынке «Хендай».

Говоря об образовании, можно отметить, что идет постоянное увеличение персонала организации, имеющего высшее образование, т.е. постоянно совершенствуется квалификация кадров.

Распределение работников в подразделении «Хендай» в ГК «Вектор» по половому признаку в 2017-2019г. показывает параллельную тенденцию увеличения численности как мужского, так и женского персонала организации. В структуре персонала компании преобладают мужчины (в 2016г. их удельный вес в структуре составил 69,87%).

Таким образом, можно сказать, что ООО «Вектор» относится к числу организаций, на которых нет половой дискриминации. Она обеспечивает работой как мужское, так и женское население.

Таким образом, в подразделении «Хендай» ГК «Вектор» работает

большое количество сотрудников, имеющих доступ к конфиденциальной информации, которая может быть отнесена к коммерческой тайне. Особое внимание необходимо уделить сотрудникам центрального офиса, как специалистам имеющим доступ к большому числу правовой, экономической и стратегической информации. Центральный офис аккумулирует информационные потоки со всех подразделений, проводит ее обработку, хранение и анализ. Что создает предпосылки к возможным злоупотреблениям со стороны сотрудников. Осуществим анализ рисков информационной безопасности.

2.2. Оценка эффективности практики защиты конфиденциальной информации организации и выявленные в ней недостатки

Обеспечение кадровой безопасности это, по сути, процесс минимизации рисков, связанных с возможным негативным воздействием кадровой составляющей корпоративных ресурсов на комплексную безопасность компании.

Для обеспечения наибольшей эффективности обеспечения кадровой безопасности, комплексная работа по обеспечению кадровой безопасности должна быть разделена на три основных этапа, смотрите рисунок 6.

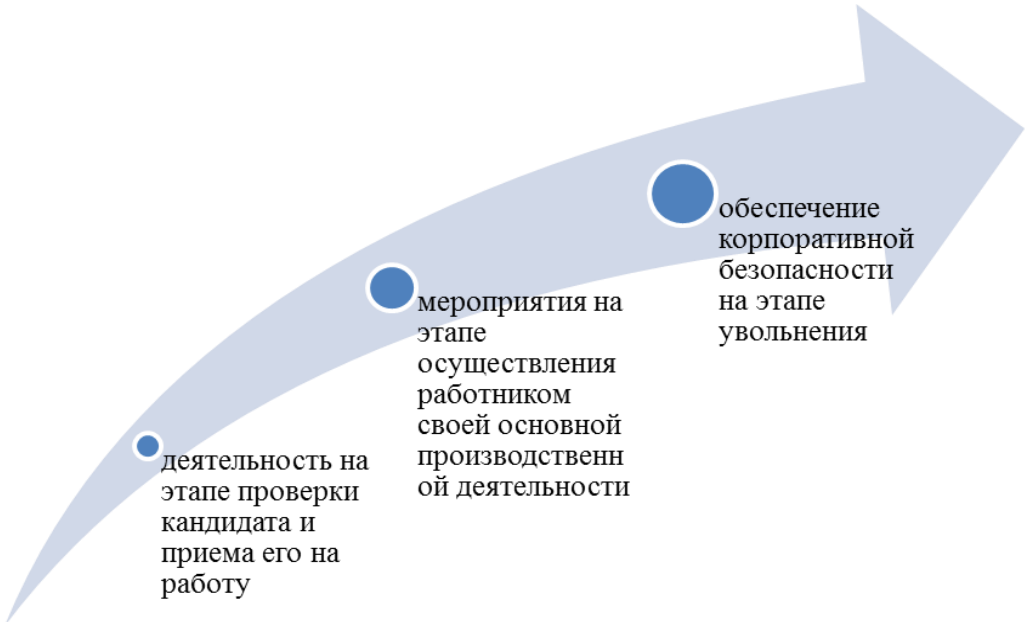


Рисунок 6– Этапы работы над обеспечением кадровой безопасности в организации

Наиболее ответственный этап это процесс прохождения кандидатом комплексной проверки на стадии приема на работу. Это естественно, чем более тщательно изучен нами кандидат с позиции корпоративной безопасности, тем меньше вероятность проникновения в компанию лиц с различными деструктивными намерениями, недостаток информации о кандидате может привести к очень неприятным для работодателя последствиям.

Здесь основной недостаток – отсутствие четких регламентов взаимодействия между службой безопасности и кадровым подразделением. HR служба не имеет представления о том, что может и что должна делать служба безопасности[24] для проверки персонала на стадии приема на работу, склонен к формализации процесс приема на работу. Зачастую кадровая служба пытается оправдать свое нежелание или неумение собрать и проверить объективную информацию о кандидате на работу законом № 152-фз о персональных данных, и слишком широко трактуют отдельные его положения. Некоторые сотрудники кадровых подразделений не ориентированы на проверку кандидатов и довольствуются лишь той информацией, которую им сообщил о себе кандидат в резюме и записями в трудовой книжке. В основном это касается приема на работу персонала на должности исполнителей (менеджеров доп. офисов или кредитных [25] специалистов на местах в торговых точках). С одной стороны, таких специалистов можно понять: на них возложена масса других обязанностей и зачастую им просто не хватает времени для качественной отработки кандидатов, вот они и пытаются таким образом оправдать свое бездействие в этом направлении работы.

Но с точки зрения обеспечения корпоративной безопасности такое положение дел недопустимо, получается, что в компанию могут попасть

[25] Мак-Мак В. Служба безопасности предприятия. – М.: Баярд, 2003. – 56с.

любые недоброжелатели, алкоголики, кадровый балласт и т.д. Последствия такого кадрового отбора крайне плачевны.

Есть и другое направление так называемой кадровой политики, если кандидата не разит за версту перегаром, в трудовой книжке все более-менее прилично и квалификация вроде бы соответствует требуемой, то его можно смело принимать на работу, а там испытательный срок покажет. Вроде удобная позиция, но с точки зрения корпоративной безопасности – крайне рискованная. Хорошо еще, если такой работник окажется просто кадровым балластом, хотя и такую категорию непутевых сотрудников увольнять бывает весьма непросто. А если человек устроился в вашу компанию по заданию спецслужбы недобросовестных конкурентов или рейдерского формирования? Трехмесячного испытательного срока ему будет вполне достаточно для выполнения шпионских заданий. Подвержены вербовочным устремлениям все, кто располагает доступом к конфиденциальной информации, активам и ресурсам компании, любой ценный сотрудник. И перечень таких рисковых должностей должен быть составлен отдельно.

Вопрос кадровой безопасности заключается в оценке, самих сотрудников, насколько они сами по своим морально-нравственным качествам устойчивы или предрасположены к такой вербовке. Низкая устойчивость и моральная готовность к негативному поведению на фоне осведомленности о коммерческих секретах, вот материал для анализа и немедленных организационных мероприятий руководства компании.

Кратко о сути взаимодействия службы безопасности и кадровой службы. Кадровая служба собирает как можно больше исходной информации о кандидате, которая станет базовой для последующей проверки и передают ее в службу безопасности; Кадровой службе нужно будет подготовить ответы на такие вопросы службы безопасности, как:

- Откуда появился этот кандидат (найден рекрутинговым агентством, обратился сам, рекомендован кем-то из действующих сотрудников и т. д.).

- Является ли претендент единственным кандидатом на вакантную должность.
- Какое первое впечатление произвёл кандидат на сотрудника службы персонала и на своего потенциального руководителя.
- Не замечены ли у претендента попытки приукрасить информацию о себе или сообщить явно ложную.
- Не выявлены ли признаки подделки представленных кандидатом документов, в частности - трудовой книжки, диплома, справки об отсутствии медицинских противопоказаний и т. д.
- Каковы перспективы кандидата в случае приёма на работу (руководящая должность после прохождения испытательного срока, самостоятельный участок работы, работа с наличными денежными средствами, доступ к конфиденциальной информации и т. д.).
- Одновременно с этим будущий руководитель проверяет профессиональные качества и убеждается в его профессиональной компетентности;
- После этого досье кандидата передается в службу безопасности, сотрудники которой проводят проверку легальными методами, после чего выдают свое заключение о целесообразности или нецелесообразности приема на работу данного кандидата.

Особым этапом проверки кандидата является его обследование с использованием полиграфа. Практика убедительно показала, что полиграф незаменим при изучении личности кандидата на работу, ибо никто не знает человека лучше, чем он сам. Проводить такое обследование целесообразно после того, как сотрудник службы безопасности провел с кандидатом собеседование (у службы безопасности могут возникнуть определенные сомнения, которыми он поделится со специалистом-полиграфологом). Само по себе включение полиграфа в систему проверки отбивает охоту попытаться проникнуть в компанию лицам с деструктивными личностными установками.

Забывают о необходимости проводить мероприятия по обеспечению кадровой безопасности на этапе профессионального функционирования работника. Сотрудники службы безопасности не задумываются о том, что представляет собой отдельно взятый работник компании на длительном этапе его производственного функционирования с точки зрения угроз компании и кадровых рисках.

Особенно это касается кредитных специалистов на местах в торговых точках, где по сути сотрудник находится без присмотра и выдача кредита на товар проходит только под контролем программы скоринг, которую легко обмануть.

Обычно считается, что на этом этапе вся ответственность за работника ложится на плечи его непосредственного начальника. Отчасти это верно, но только лишь отчасти. Руководителя подразделения интересует лишь выполнения плана и иногда вопросы трудовой дисциплины. Руководитель убежден, что ловить мошенников – дело службы безопасности, повышать уровень лояльности прямая задача кадровой службы, а от него требуется только выполнения плана любой ценой. При таком подходе кадровик появиться только в подразделении лишь тогда, когда потребуется заручиться подписью сотрудника, сотрудник безопасности, когда уже наступит кадровая угроза.

Конечно за каждым следить не нужно, под контролем службы безопасности и кадровой службы должны находиться те сотрудники, которые в силу своих функциональных обязанностей имеют доступ к конфиденциальной информации организации, а так же категория работников, представители которой могут и не иметь доступа к конфиденциальной информации, но которые в силу своего неформального авторитета способны раскачивать лодку или, наоборот стабилизировать обстановку в коллективе. Если такого неформального лидера удалось склонить на сторону администрации, то он, внешне оставаясь выразителем воли и чаяний трудовых масс, на деле становиться агентом влияния и действует в интересах

собственника компаний. Даже если такой неформальный лидер и не согласился сотрудничать, с точки зрения кадровой безопасности польза от его существования несомненная. Эти люди не только могут глаголом жечь сердца людей, но и сами объективно являются индикаторами настроений, стихийно вызревающих в трудовом коллективе. Поэтому контроль над поведением этих людей наиболее эффективный и надежный способ контроля над господствующим в коллективе настроением.

Немаловажный вопрос: а кто должен осуществлять постоянный мониторинг этих двух категорий работников (потенциальных мошенников и неформальных лидеров)? Вряд ли будет толк из того, что каждому из них будет приставлен личный куратор из службы безопасности или службы персонала. Даже неспециалисту понятно, что такое наблюдение должно быть ненавязчивым, постоянным и объективным. Сам собой напрашивается ответ - осуществлять такое наблюдение должны работники компании входящие в круг общения (желательно ближний) наблюдаемого объекта и готовые негласно информировать заинтересованные службы о поведении своих подопечных.

Тут автор подошел к еще одной проблеме – вопросам информационного обеспечения кадровой безопасности. Не будем пускаться в бессмысленные споры о приемлемости/неприемлемости донесение руководителю о своих коллег, примем как аксиому положение о том, что без получения информации о подлинном состоянии дел в коллективе обеспечить приемлемый уровень кадровой безопасности невозможно. Получить эту информацию можно лишь от той части наиболее лояльных компании членов коллектива, которые находятся в самом центре информационного пространства. Назовите их как угодно: агентами, стукачами, информаторами это роли не играет. Главное, что без помощи этих работников ни сотрудник службы безопасности, ни кадровик не могут с чистой совестью сказать, что они полностью соответствуют занимаемой должности и справляются со своими обязанностями.

Обычно этот участок работы поручается сотрудникам службы безопасности, т.к. зачастую они – выходцы из силовых структур и ранее могли иметь опыт подобной деятельности, их работа по предупреждению и выявлению внутреннего мошенничества или попыток корпоративного шпионажа предполагает приобретение таких источников информации. Но встречаются и ситуации, когда из-за отсутствия или некомпетентности службы безопасности вопросы обратной информационной связи возлагаются на плечи кадровиков.

Незаменимая такая информационная подсветка коллектива и на завершающей стадии взаимоотношений между администрацией и работником на стадии увольнения. Но здесь, с точки зрения кадровой безопасности, должны рассматриваться не только потенциальные расхитители, которые вполне могут совершить типичное хищение на прощание. Мероприятия кадрового риск-менеджмента должны коснуться и еще одной категории работников – так называемых секретоносителей. Чем ранее служба безопасности и кадровая служба узнают о намерениях этих работников прекратить свои трудовые отношения с нынешним работодателем, тем спокойнее с точки зрения корпоративной безопасности пройдет процесс.

Ни для кого не секрет, что очень часто увольняемые норовят прихватить с собой какой-то кусок материальной или интеллектуальной собственности своего работодателя. Материально ощутимые ценности позволят ему повысить свой жизненный уровень, а интеллектуальную конфиденциальную информацию (клиентская база, ноу-хау и т.п.) повысят потенциальную ценность бывшего сотрудника в глазах нового работодателя. И вот такой замысливший уволиться работник приступает к осуществлению своих замыслов. Как правило, он еще не афиширует своих намерений, но в его поведении начинают проскальзывать определенные аналитические признаки, которые, будучи тщательно систематизированными и осмысленными, дадут представление об истинных намерениях работника.

Например, если он вдруг начал интересоваться теми процессами или информационными массивами, которые ранее были ему безразличны и не входят в круг его функциональных обязанностей, что-то скачивается на накопители, ксерокопируются, фотографируется и т.д.

Может возникнуть вопрос, а как сотрудник службы безопасности или кадровик узнают об этих тревожных признаках? Никак, кроме как от своих заранее привлеченных к сотрудничеству и обученных информаторов.

Но, конечно, значительная доля ответственности здесь лежит и на непосредственном руководителе увольняющегося. Именно он в силу своих прямых служебных обязанностей должен незамедлительно проинформировать об этих тревожных признаках служба безопасности и кадровиков. Главное здесь – своевременность взаимного информирования. Обладая запасом времени, сотрудники службы безопасности и кадровики будут иметь возможность эффективно противостоять попыткам похищения конфиденциальной информации организации. Если же такой работник заранее смог скопировать всю нужную ему информацию и спокойно вынести ее за территорию, а лишь потом открыто объявил о своем желании уволиться, никаких возможностей противостоять этому желанию уже быть не может. Такое положение дел свидетельствует об одном: ни служба безопасности, ни кадровики, ни непосредственный руководитель не соответствуют занимаемой должности и вполне заслуживают наказания.

Таким образом, вопросы кадровой безопасности должны решаться совместными усилиями службы безопасности, кадровых аппаратов и линейных подразделений.

Таблица 8

Перечень сведений конфиденциального характера в подразделении «Хендай» в ГК «Вектор»

Наименование сведений	Гриф конфиденциальности	Нормативный документ

Наименование сведений	Гриф конфиденциальности	Нормативный документ
Сведения, раскрывающие характеристики средств защиты информации ЛВС организации от несанкционированного доступа.	Для служебного использования	Федеральный закон от 27.07.2006 N 149-ФЗ[26]
Требования по обеспечению сохранения служебной тайны сотрудниками организации.	Для служебного использования	Гражданский кодекс РФ [27]
Персональные данные сотрудников	Конфиденциально	Федеральный закон 152-ФЗ[28]

Кроме того, организация может устанавливать собственные пределы конфиденциальности информации (например «малая», «средняя» и «высокая»). Данные пределы необходимо оценить по выбранным критериям.

В Приложении 16 представим наиболее используемую и важную информацию.

Информация, имеющая наибольшую ценность:

1. Программное обеспечение
2. Сервера
3. Документы
4. Доступ к информационным ресурсам

Угрозы конфиденциальной информации указаны в таблице Приложение 4.

Результаты оценки угроз информационной безопасности указаны в Приложении 5.

В организации ООО «Вектор» существует 2 сети: открытая и закрытая.

Также, в организации ООО «Вектор» существуют постоянные работы с различными предприятиями, фирмами и компаниями, относящиеся к назначенной отрасли за организацией. С ними ведутся разговоры по

[26] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.07.2016) "Об информации, информационных технологиях и о защите информации"// "Российская газета", N 165, 29.07.2006
[27] "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.08.2016)// "Собрание законодательства РФ", 05.12.1994, N 32, ст. 3301
[28] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015)// "Российская газета", N 165, 29.07.2006

телефону, а также принимают и отправляют документы по факсу. Частичная схема сети показана на рисунке 7.

Закрытая сеть не имеет связи с открытой сетью, что делают компьютеры, закрытой сети, абсолютно защищенными для угроз из интернета, однако это не делает данную сеть абсолютно защищенной.

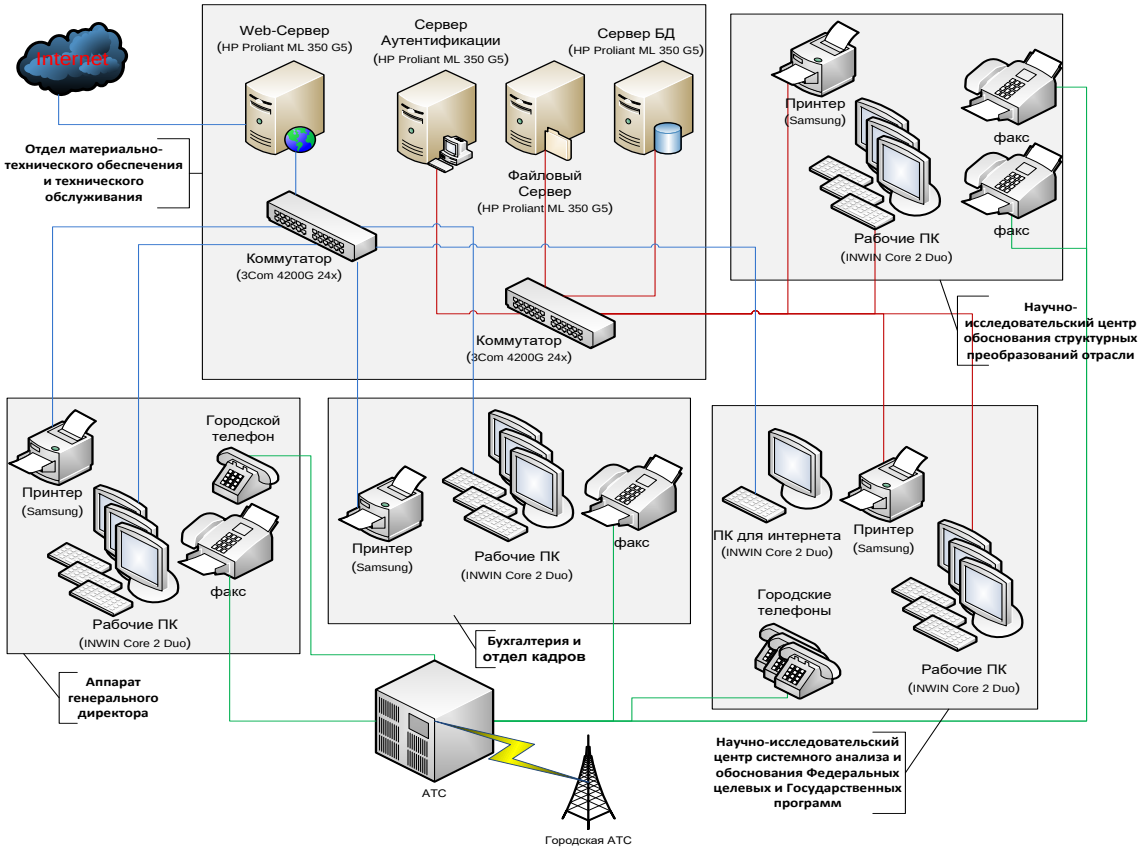


Рисунок 7 - Основная часть технической архитектуры организации ООО «Вектор»

Гостехкомисс[29] России «Средства вычислительной техники, защита информации от несанкционированного доступа к информации, показатели защищенности от несанкционированного доступа к информации» по 3 классу защищенности, «Защита от несанкционированного доступа к информации», программное обеспечение средств информации, классификация по уровню контроля отсутствия недекларированных возможностей» по 2 уровню контроля.

Кроме того, в ООО «Вектор» расположен свой Web-Сервер с размещенным на нем сайтом предприятия. Данный сервер кроме сайта

[29] Официальный сайт компании Страж NT [Электронный ресур]: http://www.guardnt.ru/

раздает интернет, с помощью прокси-сервера, на некоторые устройства в открытой сети, также обеспечивает деятельность почтового клиента MS Outlook. Web-Сервер также осуществляет обновление БД антивируса.

Неполная программная архитектура организации ООО «Вектор» представлена на рисунке 7.

По программной архитектуре организации ООО «Вектор» автор может увидеть, что организация использует в качестве БД MS SQL Server и для совместимости со старой системой хранилище для DBF-файлов. Они установлены на web-сервере БД, с программной защитой системы «Страж NT», что дает возможность подключения к ней только со специального программного обеспечения, установленного в той же сети. С целью ускорения взаимодействия между работниками разных отделов был создан и оптимизирован Файловый Сервер.

Другой способ передачи информации происходит за счет передачи информации на съемных носителях, заранее прописанные как разрешенные на использование в системе Страж NT, однако данные с грифом «секретно» автоматически шифруются и могут в дальнейшем быть прочтены лишь данной системой. Однако, это не исключает риск халатности работников, имеющих доступ к конфиденциальным данным, которые могут намеренно или случайно пометить конфиденциальные данные в документе как не конфиденциальные.

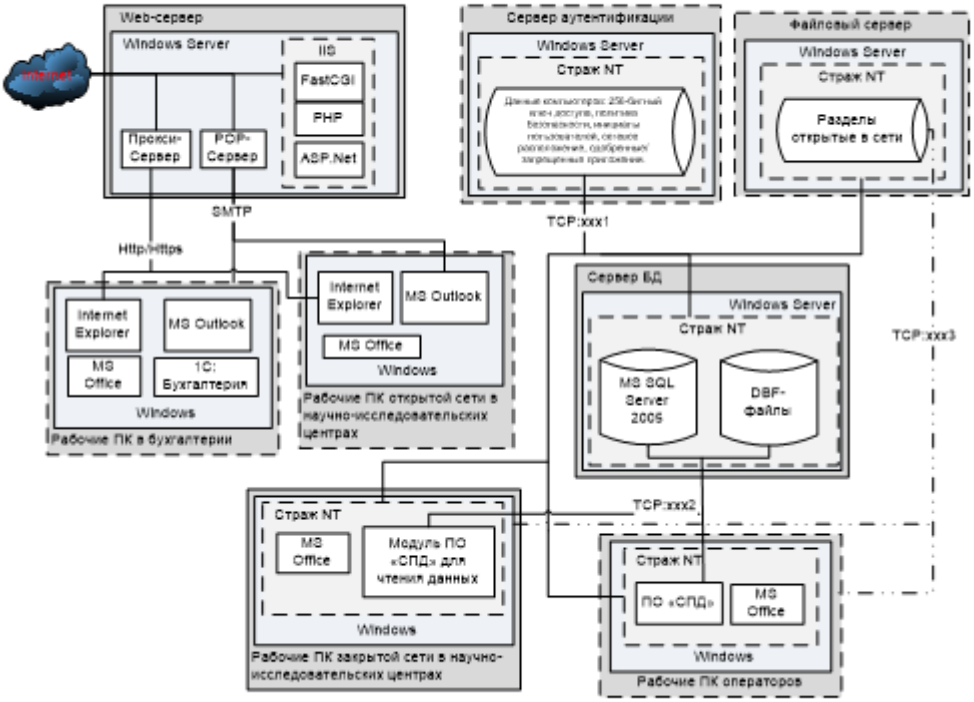


Рисунок 8 - Основная часть программной архитектуры организации ООО «Вектор»

В некоторых отделах ООО «Вектор» закрытой сети расположен компьютер для отправки и получения по электронной почте писем, которые не имеют грифа «секретности».

ООО «Вектор» снимает помещения у другой организации, которая должна обеспечивать защищенность этажей от проникновения посторонних лиц. Но, в здании находятся и другие организации, также снимающие помещения, и оформляющие заявки на пропуск посторонних лиц, что не уменьшает степень угрозы. Необходимо отметить, что обслуживающий персонал является работниками другой организации, но в здании с паролем они имеют доступ только тогда, когда их пропускают туда сотрудники, которые работают в этих отделах.

Сетевые кабели ООО «Вектор» проведены по специальным каналам, которые находятся в потолке коридора. За исключением установленных

камеры, это делает их достаточно уязвимыми для подключения к сети. Все же, на закрытую сеть одного только подключения извне недостаточно.

В Приложении 6 изображен один из этажей здания с отображением дверей с кодовыми замками на дверях и показом размещения камер видеонаблюдения. Данный рисунок, демонстрирует нам, обзор камер охватывающих весь коридор, что в свою очередь дает возможность в любое время выяснить, кто и когда входил в здание.

Понятие информационной безопасности неразрывно связано с рисками для информационных ресурсов, под которыми понимается возможность нанесения ущерба информационным ресурсам, снижения уровня их защищенности.

Приложение 11 содержит анализ основных задач по обеспечивающих информационную безопасность предприятия ООО «Вектор».

Для базовой оценки рисков достаточно шкалы оценки критичности из трех уровней - низкий, средний и высокий. В таком случае оценка каждого уровня в денежном эквиваленте будет выполняться на основе определенных принципов.

Пример трехуровневой шкалы с оценкой в денежных единицах представлен в приложении 12.

1. Программное обеспечение, материальные ресурсы и сервисы оцениваются, как правило, с точки зрения их доступности или работоспособности. Например, последствия неработоспособности системы кондиционирования на протяжении трех суток является отказ серверов компании, к этим серверам будет нарушен доступ, из-за чего организация понесет убытки;

2. Сотрудники компании с точки зрения конфиденциальности и целостности оцениваются, учитывая их доступ к информационным ресурсам с правами на чтение и на модификацию.

3. Репутация компании оценивается в связи с информационными ресурсами.

4. Оценка риска является оценкой соотношения возможных негативных воздействий на деятельность организации при наступлении нежелательных инцидентов и уровня оцененных угроз, а также уязвимых мест. Риск же является фактически мерой уязвимости системы и связанной с ней организации. Величина риска зависит от:

- ценности информации;
- легкости реализации угроз в уязвимых местах с оказанием нежелательного воздействия;

Ценность информации определяется на основе оценок их владельцев, специалиста по ИТ. Угрозы и уязвимые места определяются ИТ-специалистами.

На данный момент существует ряд методов оценки риска. Важно, чтобы организация пользовалась самым удобным и доверенным методом, который приносит воспроизводимые результаты.

Оценка рисков производится экспертным путем на основании анализа ценности активов, вероятности реализации угроз и использования незащищенностей, о которых говорилось в предыдущих пунктах (Рисунок 8).

	Уровни угрозы	Низкая			Средняя			Высокая		
	Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Ценность активов	1	*0*	*1*	*2*	*1*	*2*	*3*	*2*	*3*	*4*
	2	*1*	*2*	*3*	*2*	*3*	*4*	*3*	*4*	*5*
	3	*2*	*3*	*4*	*3*	*4*	*5*	*4*	*5*	*6*
	4	*3*	*4*	*5*	*4*	*5*	*6*	*5*	*6*	*7*
	5	*4*	*5*	*6*	*5*	*6*	*7*	*6*	*7*	*8*

Рисунок 9 - Уровень угроз и уязвимостей

При определении уровня незащищённости из результатов аудита или самостоятельной оценки для различных процессов (Приложение 18).

Краткие выводы по главе

В ходе написания второй главы, которая была посвящена практике противодействиям угрозам информационной безопасности организации ООО «Вектор» со стороны собственного персонала, автор пришел к следующим выводам:

1. Объектом исследования выступает подразделение Группы компаний «Вектор», курирующего работу с марками автомобиля «Хендай» - ООО «Вектор-Трейд», расположенного по адресу: Российская Федерация, 107497, город Москва, улица Иркутская, дом 5/6, строение 1, помещение 321.

2. Основной сферой деятельности компании является продажа новых иномарок. Вектор представляет 21 автомобильную марку – Nissan, Volkswagen, Renault, Opel, Infiniti, Chevrolet, KIA, Hyundai, Mazda, Škoda, Toyota, Ford, Cadillac, Suzuki, Citroën, Datsun, Mitsubishi, SsangYong, Peugeot, Lada и УАЗ.

3. Компания объединяет 48 дилерских центров: 19 в Москве, 26 – в регионах (Санкт-Петербург, Брянск, Воронеж, Самара, Ярославль, Челябинск, Екатеринбург, Новосибирск, Архангельск, Сургут, Новокузнецк, Саратов и Краснодар) и 3 – в Казахстане (Астана, Алматы, Караганда). По итогам 2015 года доля федерального рынка компании Вектор составила 2.9%, доля столичного рынка – 6.5%. В штате компании более 6 000 сотрудников. Таким образом, предприятие ГК «Вектор» является активно развивающимся предприятием, с разветвленной филиальной сетью. Такое построение бизнеса требует организации системы информационного обеспечения, защищенного от возможных рисков, в том числе и со стороны злоупотребления персоналом.

4. В подразделении «Хендай» ООО «Вектор» работает большое количество сотрудников, имеющих доступ к конфиденциальной информации, которая может быть отнесена к коммерческой тайне. Особое внимание необходимо уделить сотрудникам центрального офиса, как

специалистам имеющим доступ к большому числу правовой, экономической и стратегической информации. Центральный офис аккумулирует информационные потоки со всех подразделений, проводит ее обработку, хранение и анализ, что создает предпосылки к возможным злоупотребления

5. Но не все гладко во взаимодействии службы персонала, службы безопасности и непосредственных руководителей сотрудников. Особо это проявляется при найме молодых сотрудников на должности специалистов на места в торговых точках. Ввод полиграфа при найме сотрудника в принципе решает эту проблему, но не совсем устраняет ее. Так же присутствует проблема в отсутствии должного контроля над сотрудниками во время выполнения должностных обязанностей.

6. Вопросы кадровой безопасности должны решаться совместными усилиями служба безопасности, кадровых аппаратов и линейных подразделений во время работы сотрудников, а не только при найме и увольнении сотрудников.

7. Проведенный нами анализ системы информационной безопасности ООО «Вектор» выявил существенные проблемы, в числе которых: резервный сервер находится в одном помещении с основными серверами, хранение резервных копий в серверной,; отсутствие необходимых правил в отношении парольной защиты; администрированием сети занимается один человек.

Глава 3. Рекомендации по повышению степени защищенности организации ООО «Вектор» от рассматриваемых угроз

3.1. Защита конфиденциальной информации в электронной форме

Проведенный нами анализ системы информационной безопасности ООО «Вектор» выявил существенные недостатки в защите информации в электронном виде, к которым относится:

- отсутствие надлежащих правил в отношении парольной защиты;
- администрированием сети занимается один человек;
- хранение резервных копий в серверный, резервный сервер находится в одном помещении с основными серверами.

Обобщение международной и российской практики в области управления безопасностью конфиденциальной информации в организации позволило заключить, что для ее обеспечения необходимы следующие условия, смотрите рисунок 10.

Рисунок 10 – Условия для обеспечения безопасности конфиденциальной информации в ООО «Вектор»

В связи с этим, автор рекомендует применить систему Data Loss Prevention, находящую и блокирующую несанкционированную передачу конфиденциальной информации в электронном виде по любому каналу с использованием информационной структуры.

Главная задача системы Data Loss Prevention - это минимизация риска утечки или уничтожения конфиденциальной информации, промышленного шпионажа, халатности и других неправомерных действий персонала организации.

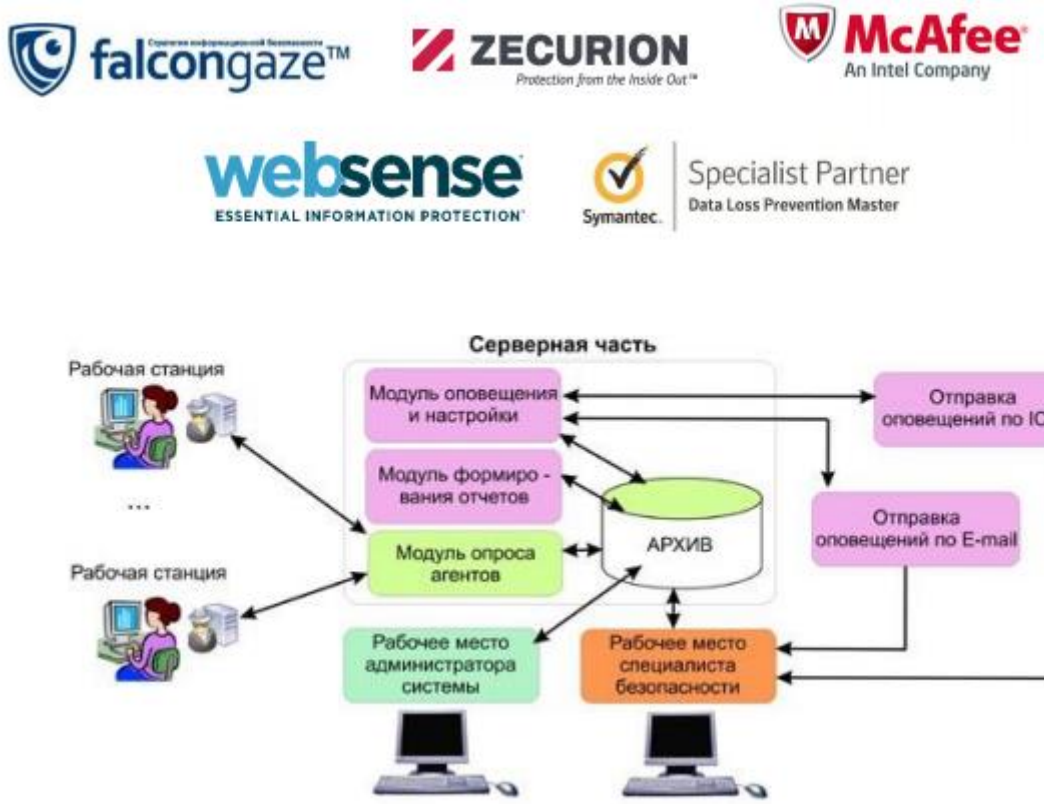


Рисунок 11 – Принципы работы систем Data Leakage Prevention для защиты конфиденциальной информации

Существуют различные подходы к классификации Data Loss Prevention-систем. Так, с точки зрения архитектуры существуют шлюзовые и хостовые решения, а с точки зрения предотвращения утечек — активные и пассивные. Классификация важна для сравнения Data Loss Prevention примерно одного уровня и выбора для внедрения наилучшего решения.

Более-менее сложившееся представление рынка указывают на наличие общих ключевых характеристик, которые позволяют отнести информационно-безопасные решения к классу Data Loss Prevention.

Система Data Loss Prevention осуществляет следующие функции, смотрите рисунок 12.

Рисунок 12 - Функции системы Data Loss Prevention осуществляет

Zecurion Data Loss Prevention — комплексная система защиты от утечек корпоративной информации. Zecurion Data Loss Prevention является наиболее технологичным решением на рынке в сравнении с Data Loss Prevention -системами конкурентов по состоянию на 2011 год, а сама компания Zecurion — лидером среди всех Data Loss Prevention -вендоров по объемам выручки.

Zecurion Data Loss Prevention позволяет имеет контроль над корпоративной электронной почтой, письмами и вложениями, отсылаемыми через сервисы , сообщениями интернет-мессенджеров, FTP, POP3, IMAP,

SMTP и другими сетевыми каналами, файлами, записываемыми на USB-накопители и любые внешние устройства, печатью на локальных и сетевых принтерах, наличием конфиденциальных данных, хранящимися на компьютерах пользователей и серверах, доступом к информации, которая хранится на серверах, магнитных лентах и оптических дисках.

К основным преимуществам комплекса Zecurion Data Loss Prevention относят: борьбу и контроль утечек информации, гибридный анализ перехваченных данных с использованием морфологии, «цифровых отпечатков», регулярных выражений, OCR и собственной технологии SmartID, поддержку анализа более 500 типов файлов, блокирование утечек в режиме реального времени, архивирование всей перехваченной информации, возможности последующего поиска и анализа данных архива, сканирование сетевых и локальных хранилищ для поиска файлов с конфиденциальной информацией, защиту данных в местах хранения, единый консоль управления.

По мнению автора, в результате применения комплекса Zecurion Data Loss Prevention передача конфеденциальной информации в электронном виде в ООО «Вектор» окажется под полным контролем (смотрите Рисунок 13):

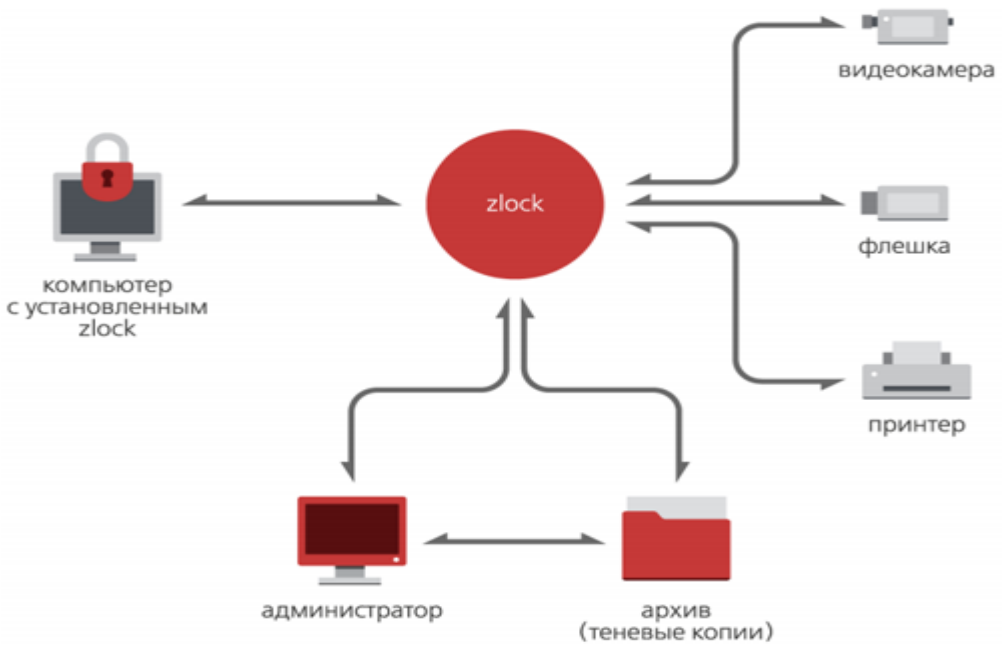


Рисунок 13 – Алгоритм работы систем Data Leakage Prevention с помощью Zecurion DLP в ООО «Вектор»

Сегодня мобильность сотрудника организации играет важную роль в логике ведения бизнеса. Ипользование персоналом организации ООО «Вектор» корпоративных смартфонов и планшетов, также, повышает эффективность их работы на десятки процентов.

Следующей важной рекомендацией, по мнению автора, является отслеживание коммуникативных связей между сотрудниками организации, выявление неформальных лидеров в коллективе, кроме того контролирование процесса коммуникации работников ООО «Вектор» с бывшими сотрудниками. Для сотрудников службы безопасности в выявлении конкретных работников, которые осуществляют разглашение конфиденциальной информации.

На основании анализа практики ситуаций, связанных с угрозми небезопасности конфиденциальной информации со стороны его сотрудников, определенна «группа риска», к которой следует отнести следующие категории работников ООО «Вектор»:

3.2. Защита конфиденциальной информации на бумажных носителях

Касательно практики защиты конфиденциальной информации на печатных носителях, то их контроль технически сложнее, чем электронных. После выхода бумажного документа из принтера следить за ним можно лишь «вручную», с помощью специально обученных работников и организационных процедур. В связи, с относительной дешевизной технических решений и относительной дороговизной рабочей силы, в ООО «Вектор» контролирование печатных носителей технически слабее контролирования компьютерной информации.

С целью снижения числа «бумажных» утечек и повышения уровня защиты конфиденциальной информации на печатных носителях, автор

считает целесообразным реализовать мероприятия по следующим направлениям, рисунок .

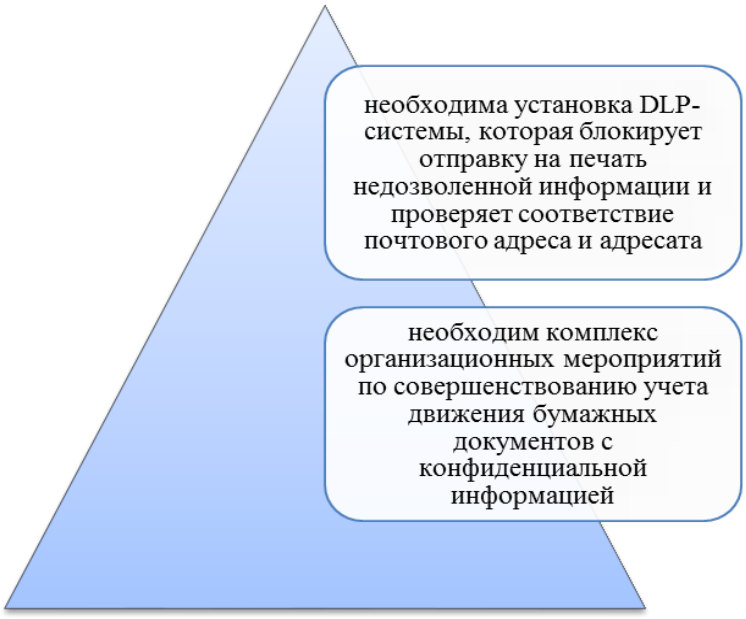


Рисунок 14 - Рекомендуемые мероприятия для снижения числа «бумажных» утечек и повышения уровня защиты конфиденциаьной информации на печатных носителях

Кроме того, автор считает, что целесообразно применить в ООО «Вектор» DLP-приложение PrintControll.

К преимуществам системы относят: контроль над содержимым всех распечатанных в ООО «Вектор» документов, возможность отслеживания утечек документов в случае попыткок их хищения в бумажном виде; оценку целесообразности использования принтера каждым работников ООО «Вектор»; анализ содержимого всех напечатанных документов; создание электронного архива распечатанных документов; использование агентов на рабочих станциях, дающих возможность контролировать не только сетевые принтеры, но и печатные устройства, используемые локально; встроенную систему оптического распознавания текста на изображениях.

Автор считает, что в состав принципов процесса организации учета движения бумажных документов с конфиденциальной информацией в ООО «Вектор» уместно добавить следующие принципы, рисунок 15.

принцип комплексности	при построении системы защиты учетных данных необходимо предусматривать проявление всех видов возможных угроз для компании, включая каналы несанкционированного доступа к конфиденциальной информации на печатных носителях, и все возможные для него средства защиты
принцип безопасности и контроля данных	предусматривает защиту ценной печатной информации, путем установления ограничения пользователей, отнесения ее к информации конфиденциального характера и введения ограничений при работе с ней
принцип адекватности	применение вышеуказанных мер защиты нужно сопоставлять с возможными видами угроз, а средства защиты информации на печатных носителях должны функционировать в рамках единого комплекса защиты конфиденциальной информации ООО «Вектор», взаимно дополняя друг друга в функциональном и техническом аспектах

Рисунок 15 - Принцип процесса организации учета движения бумажных документов в ООО «Вектор»

Ответственность за защиту данных на печатных носителях, которые составляют коммерческую тайну, по мнению автора следует возлагают не только на службу безопасности, но и на весь управленческий персонал ООО «Вектор» - от руководителя до технического персонала.

С целью минимизации риска утечки конфиденциальной информации на бумажных носителях в ООО «Вектор», по мнению автора, необходимо принимать соответствующие меры, классифицируя их в соответствии с определенными угрозами, приложение 19.

3.3. Защита конфиденциальной информации в устной форме

Исходя из проведенного нами исследования защиты конфиденциальной информации в устной форме, по мнению автора, персонал ООО «Вектор» должен соблюдать следующие меры по обеспечению информационной безопасности:

- По возможности не допускать нахождение посторонних лиц в помещениях, в которых ведутся работы с секретной и конфиденциальной

информацией. Если же посторонние лица оказались допущены (сотрудники, которые не относящиеся к данной организации или сотрудники, не обладающие требуемым уровнем доступа), то необходимо бдительно следить за ними, для того чтобы избежать несанкционированной утечки информации.

- Пароли, для доступа в помещения, должны знать исключительно администраторы и работники этого отдела. Двери с кодовыми замками должны быть всегда закрытом состоянии. Исключением являются, случи, когда в помещении присутствуют работники, не имеющие отношения данному отделу.
- Печатные документы с конфиденциальной информацией должны храниться только в 1 отделе, остальные документы должны храниться в отведенном для этого месте.
- Интернет должен использоваться только для работы.

Разработанный нами план, по реструктуризации ключевых факторов сохранения информационной безопасности в помещениях включает в себя:

- размещение камер в помещениях, в которых хранятся базы данных, документы и другие ценные ресурсы организации;
- обеспечение безопасности от угроз считывания побочных электромагнитных излучений.

Для решения задач, описанных в п.п. 1.3.1 необходимо совершить закупку и установку следующих устройств: камер, видеорегистраторов, а также генераторов шума. Рассмотрим рынок данных устройств:

Видеокамеры (Приложение 7)

Видеорегистраторы (Приложение 8)

Генераторы шума (Приложение 9)

Для решения наших задач следует закупить видеокамеры, видеорегистраторы и генераторы шума.

Рисунок 16 - Цветная купольная видеокамера AV Tech MC27

стандарт видеосигнала – PAL/NTSC
разрешение – PAL 720x576, 720x288, 360x288 / NTSC 720x480, 720x240, 360x240
технология сжатия – H.264 (MPEG4 - 10PART), аппаратное сжатие в реальном времени. Динамическое сжатие = 40:1 - 2400:1
видеовход – BNC x 16 (1 Vp-p композитный / 75 Ом)
видеовыход – BNC x 2, D-SUB VGAx1
аудиовход – RCA x 2 (24K bps ADPCM). Синхронизация с видеозаписью
скорость записи – 60 кадр/сек. /720x480, 120 кадр/сек. /720x240, 240 кадр/сек. /360x240 (NTSC); 50 кадр/сек. /720x576, 100 кадр/сек. /720x288, 200 кадр/сек. /360x288 (PAL
аудиовыход – RCA x 1 Синхронизация с видеозаписью
режим записи – Ручной режим/постоянная/ по расписанию/ по тревоге
управление – Кнопки на передней панели, пульт, USB-мышь (дополнительно)
поддержка жёстких дисков – Поддержка одного жесткого диска типа 3,5» SATA до 2 Тб каждый и более
режим воспроизведения – по кадрам. Ускоренное воспроизведение вперед и назад (до 64x);

Рисунок 17 – характеристики видеорегистратора для ООО «Вектор»

Функции тревоги:

1. Потеря изображения;
2. Вход датчика;
2. Отправка e-mail сообщения на стационар;

Соотношение цена/качество данного видеорегистратора оптимально подходит для его использования в подразделении «Хендай» в ГК «Вектор».

Рисунок 18 - Ai-D365 16-канальный регистратор в корпусе из сплава алюминия.

Рисунок 19 - Система защиты информации «Гром-ЗИ-4Б».

Видеорегистратор будет располагаться в комнате отдела «материально-технического обеспечения и технического обслуживания».

Рисунок 20 - Рабочий интерфейс видеорегистратора.

Рисунок 21 - Программный интерфейс видеорегистратора

Расположение данных оборудований изображено в Приложении 10.

Риск владельца информации зависит от уровня инженерно-технической защиты информации, который, в свою очередь, определяется ресурсами системы.

Данные по ресурсам необходимым для ИБ представлены в таблицах в приложении 13 и 15.

Суммарное значение ресурса, выделяемого на защиту информации исходя из расчетов, составил: 98 355 + 38 640 = 136 995 (руб.)

Таким образом, разработанный проект является эффективным и способен снизить риски потерь организации за год на 385 тыс. рублей.

Краткие выводы по главе

Для решения поставленных перед нами задач следует установить дополнительную программу контроля Zecurion DLP, закупить видеокамеры, видеорегистраторы и генераторы шума.

В отделах будет осуществляться отделом «материально-технического обеспечения и технического обслуживания».

Разработанный проект является эффективным и способен снизить риски потерь ООО «Вектор» за год на 385 тыс. рублей.

Заключение

По результатам проведенного теоретического анализа, представленного в первой главе работы, были сделаны следующие выводы.

Целью информационной безопасности является безопасность информационных ресурсов в любой момент времени и в любой обстановке.

Под безопасностью информационных ресурсов (информации) понимается относительно гарантированная в конкретной ситуации защищенность информации во времени и пространстве от любых объективных и субъективных угроз (опасностей), возникающих в обычных условиях функционирования фирмы и условиях экстремальных ситуаций.

В целом можно отметить, что информационная безопасность должна стать важнейшей частью корпоративной культуры компании, подкрепленной комплексом программно-технических и организационных мер, которые позволят минимизировать риски подобного рода.

Объектом исследования выступает подразделение Группы компаний «Вектор», курирующего работу с марками автомобиля «Хендай» - ООО «Вектор-Трейд», расположенного по адресу: Российская Федерация, 107497, город Москва, улица Иркутская, дом 5/6, строение 1, помещение 321.

Основной сферой деятельности компании является продажа новых иномарок. Вектор представляет 21 автомобильную марку – Nissan, Volkswagen, Renault, Opel, Infiniti, Chevrolet, KIA, Hyundai, Mazda, Škoda, Toyota, Ford, Cadillac, Suzuki, Citroën, Datsun, Mitsubishi, SsangYong, Peugeot, Lada и УАЗ.

Компания объединяет 48 дилерских центров: 19 в Москве, 26 – в регионах (Санкт-Петербург, Брянск, Воронеж, Самара, Ярославль, Челябинск, Екатеринбург, Новосибирск, Архангельск, Сургут, Новокузнецк, Саратов и Краснодар) и 3 – в Казахстане (Астана, Алматы, Караганда). По итогам 2015 года доля федерального рынка компании Вектор составила 2.9%,

доля столичного рынка – 6.5%. В штате компании более 6 000 сотрудников. Таким образом, предприятие ГК «Вектор» является активно развивающимся предприятием, с разветвленной филиальной сетью. Такое построение бизнеса требует организации системы информационного обеспечения, защищенного от возможных рисков, в том числе и со стороны злоупотребления персоналом.

В подразделении «Хендай» ГК «Вектор» работает большое количество сотрудников, имеющих доступ к конфиденциальной информации, которая может быть отнесена к коммерческой тайне. Особое внимание необходимо уделить сотрудникам центрального офиса, как специалистам имеющим доступ к большому числу правовой, экономической и стратегической информации. Центральный офис аккумулирует информационные потоки со всех подразделений, проводит ее обработку, хранение и анализ, что создает предпосылки к возможным злоупотреблениям со стороны сотрудников.

Разработанный проект является эффективным и способен снизить риски потерь организации за год на 385 тыс. рублей.

Литература

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.07.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.11.2017)// "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3448

2. Федеральный закон от 02.12.1990 N 395-1(ред. от 26.03.2013) «О банках и банковской деятельности». Закон РФ от 02.12.1990 N 395-1

3. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) "О персональных данных"// "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3451

4. Уголовный кодекс Российской Федерации. Федеральный закон от 13.06.1996 N 63-ФЗ (ред. от 19.04.2013)

5. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.08.2016)// "Собрание законодательства РФ", 05.12.1994, N 32, ст. 3301

6. Налоговый кодекс Российской Федерации. Часть первая. Федеральный закон от 31.07.1998 N 146-ФЗ (ред. от 04.04.2013)

7. Алексенцев А. И О классификации конфиденциальной информации по видам тайны // Безопасность информационных технологий. 1999. N 3. С. 48-53.

8. Антонов А.В. Информация: восприятие и понимание. Киев, АН УССР, 1988. С. 123-125.

9. Бачило И.Л. Информационное право: основы практической информатики. М.: Вектор,2007. С. 97.

10. Башаратьян М. К. Система конституционных прав и свобод граждан Российской Федерации в сфере деятельности средств массовой информации: дисс. ... канд. юрид. наук. М., 2007. С. 79-80.

11. Валитова Л. И. К вопросу об ограничении права на информацию // Право и государство: теория и практика. 2011. N 6. С. 32-35

12. Девянин П.Н. Садердинов А.А., Трайнев В.А. и др. «Информационная безопасность предприятия» Учебное пособие, - М., 2006.

13. Кучеренко А. В. Информация как объект правового регулирования // Вестник Амурского государственного университета. 2007. N 36. С. 39.

14. Мак-Мак В. Служба безопасности предприятия. – М.: Баярд, 2003. – 56с.

15. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. М.: Атберг-98, 2013. С. 787.

16. Омарова А. Б. Гражданско-правовые проблемы института коммерческой тайны: дисс… канд. юр. наук. М., 2001. С. 43.

17. Официальный сайт компании Страж NT [Электронный ресурс]. - Режим доступа: http://www.guardnt.ru/ (Дата обращения: 22.11.17)

18. Официальный сайт ГК «Вектор» [электронный ресурс]. - Режим доступа: http://www.vektorauto/ (Дата обращения: 22.11.17)

19. Рэдхед К. Управление финансовыми рисками на стратегическом уровне М: ИНФРА-М – 2013- с.125

20. Семашко А.В. Правовые основы оборота информации с ограниченным доступом (конфиденциальной информации) в Российской Федерации: Автореф… дисс… канд. юр. наук. М., 2008. С. 17.

21. Соколов А.В., Степанюк О.М. «Защита от компьютерного терроризма» Справочное пособие. - СПб.: БХВ - Петербург, Арлит, 2002

22. Степанов А. Г., Шерстнева О. О. Защита коммерческой тайны. М.: Альфа-Пресс, 2006. С. 34.

23. Тиновицкая И. Д. Правовая информация: законодательные проблемы // Проблемы информатизации. 2005. N 1.; Ефремов А. А. Понятие и виды конфиденциальной информации // Право и экономика. 2004. N 4: и др.

24. Фатьянов А. А. Концептуальные основы обеспечения безопасности на современном этапе // Безопасность информационных технологий. 1999. N 1. С. 26-40.

25. Шевердяев С. Н. "Конституционно-правовой режим информации ограниченного доступа". Конституционное и муниципальное право. 2007.

26. Шиверский А. А. Защита информации: проблемы теории и практики. М.: Юристъ, 1996. С. 12-13.

27. Щадрин, С. Ф. Уголовно-правовая охрана служебной тайны: Автореф… дисс… канд. юр. наук. Ростов-на-Дону,2002. С. 12-13.

28. Ярочкин, В.И. Информационная безопасность. 7-е изд. / В.И. Ярочкин. — М.: Академический проект, 2014. — 544 с.

Приложения

Приложение 1

Качественный состав трудовых ресурсов организации в 2017-2019г.

Показатель	Численность работников, чел			Удельный вес, %			Абс. откл. (2018/2017)	Отн. откл. (2018/2019),%
	2017	2018	2019	2017	2018	2019		
Группы работников								
По возрасту, лет:								
до 20	-	2	2		0,80	0,66	0	0
от 20 до 30	94	105	141	45,85	41,83	46,69	36	34,29
от 30 до 40	84	94	107	40,98	37,45	35,43	13	13,83
от 40 до 50	12	32	30	5,85	12,75	9,93	-2	-6,25
от 50 до 60	10	15	17	4,88	5,98	5,63	2	13,33
старше 60	5	3	5	2,44	1,20	1,66	2	66,67
Итого	205	251	302	100	100	100	51	20,32
По полу:								
мужчины	128	167	211	62,44	66,53	69,87	44	26,35
женщины	77	84	91	37,56	33,47	30,13	7	8,33
Итого	205	251	302	100,00	100,00	100,00	51	20,32
По образованию:								
незаконченное среднее	5	7	3	2,44	2,79	0,99	-4	-57,14
среднее, среднее специальное	43	58	47	20,98	23,11	15,56	-11	-18,97
высшее	157	186	252	76,59	74,10	83,44	66	35,48
Итого	205	251	302	100	100	100	51	20,32
По трудовому стажу, лет:								
до 5	47	48	41	22,93	19,12	13,58	-7	-14,58
от 5 до 10	105	148	173	51,22	58,96	57,28	25	16,89
от 10 до 15	39	40	72	19,02	15,94	23,84	32	80,00
от 15 до 20	14	15	16	6,83	5,98	5,30	1	6,67
свыше 20	0	0	0	0,00	0,00	0,00	0	0,00
Итого	205	251	302	100	100	100	51	20,32

Приложение 2

Оценка информационных активов организации

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная оценка	Качественная
Информационные активы						
обработка документов	Документы	Бумажный документ и электронный вид документа.	Отдел сбора и обработки статистической и бухгалтерской отчетности	Первоначальная стоимость актива		малая
обработка документов	БД компании	Электронный носитель	Отдел сбора и обработки статистической и бухгалтерской отчетности	Первоначальная стоимость актива		средняя
					Количественная оценка	Качественная
доступ к информационным ресурсам	БД компании	Электронный носитель	Отдел материально-технического обеспечения и технического обслуживания; Сотрудники научно-исследовательских центров.	Первоначальная стоимость актива		средняя

обмен корреспонденцией	Файлы электронной почты, стандарты форм, справочники, приказы	Электронный носитель	Все сотрудники	Первоначальная стоимость актива		малая
Активы программного обеспечения						
обработка документов	Офисные программы;	Электронный носитель	Сотрудники	Первоначальная стоимость актива		малая
обеспечение непрерывной работы	Системное ПО; Антивирусное ПО	Электронный носитель	Отдел материально-технического обеспечения и технического обслуживания	Первоначальная стоимость актива		средняя
					Количественная оценка	Качественная
защита данных	Страж NT	Электронный носитель	Отдел материально-технического обеспечения и технического обслуживания	Первоначальная стоимость актива		высокая
управление данными	СУБД MS SQL Server	Электронный носитель	Отдел материально-технического обеспечения и технического обслуживания	Первоначальная стоимость актива		высокая

обработка документов	ПО «СПД41»	Электронный носитель	Отдел сбора и обработки статистической и бухгалтерской отчетности	Первоначальная стоимость актива		средняя
Разработка программного обеспечения по конкурсам	Разрабатываемое ПО	Электронный носитель	Отдел разработки, внедрения и сопровождения программных средств	Первоначальная стоимость актива		высокая
Физические активы						
доступ к информационным ресурсам	Аппаратные средства (компьютеры, принтера, факсы)	Материальный объект	Сотрудники	Первоначальная стоимость актива		очень высокая
					Количественная оценка	Качественная
хранение данных	Сервера	Материальный объект	Отдел материально-технического обеспечения и технического обслуживания	Первоначальная стоимость актива		высокая

Приложение 3

Результаты оценки уязвимости активов

Группа уязвимостей Содержание уязвимости	Сервера	БД	ПО	Документы	ПК
1. Среда и инфраструктура					
Отсутствие физической защиты зданий, дверей и окон	низкая	низкая	низкая	низкая	низкая
Неправильное или халатное использование физических средств управления доступом в здания, помещения	средняя	низкая	низкая	средняя	высокая
Нестабильная работа электросети	средняя	средняя	средняя	средняя	средняя
Размещение в зонах возможного затопления	низкая	низкая	низкая	низкая	низкая
2. Аппаратное обеспечение					
Подверженность колебаниям напряжения	низкая	средняя	средняя	низкая	низкая
Подверженность температурным колебаниям	средняя	низкая	низкая	низкая	низкая
Подверженность воздействию влаги, пыли, загрязнения	средняя	низкая	низкая	низкая	низкая
Чувствительность к воздействию электромагнитного излучения	низкая	средняя	средняя	низкая	низкая
Недостаточное обслуживание/неправильная инсталляция запоминающих сред	низкая	средняя	средняя	низкая	низкая
Отсутствие контроля за эффективным изменением конфигурации	низкая	низкая	средняя	средняя	средняя
3. Программное обеспечение					
Неясные или неполные технические требования к разработке средств программного обеспечения	низкая	низкая	средняя	высокое	низкая
Отсутствие тестирования или недостаточное тестирование программного обеспечения	низкая	средняя	средняя	средняя	средняя
Сложный пользовательский интерфейс	низкая	низкая	средняя	высокая	низкая
Отсутствие механизмов идентификации и аутентификации, например аутентификации пользователей	низкая	средняя	низкая	низкая	низкая

Отсутствие аудиторской проверки	низкая	низкая	низкая	низкая	средняя
Хорошо известные дефекты программного обеспечения	низкая	низкая	низкая	низкая	низкая
Незащищенные таблицы паролей	низкая	низкая	низкая	низкая	низкая
Плохое управление паролями	низкая	низкая	низкая	низкая	низкая
Неправильное присвоение прав доступа	низкая	низкая	низкая	низкая	низкая
Неконтролируемая загрузка и использование программного обеспечения	низкая	низкая	низкая	средняя	средняя
Отсутствие регистрации конца сеанса при выходе с рабочей станции	низкая	низкая	низкая	низкая	низкая
Отсутствие эффективного контроля внесения изменений	низкая	низкая	средняя	средняя	низкая
Отсутствие документации	низкая	средняя	средняя	средняя	низкая
Отсутствие резервных копий	низкая	низкая	средняя	средняя	низкая
Списание или повторное использование запоминающих сред без надлежащего стирания записей	низкая	низкая	низкая	низкая	низкая
4. Коммуникации					
Незащищенные линии связи	низкая	низкая	низкая	средняя	низкая
Неудовлетворительная стыковка кабелей	низкая	низкая	низкая	низкая	низкая
Отсутствие идентификации и аутентификации отправителя и получателя	низкая	низкая	низкая	низкая	низкая
Пересылка паролей открытым текстом	низкая	низкая	низкая	низкая	низкая
Отсутствие подтверждений посылки или получения сообщения	низкая	низкая	низкая	средняя	низкая
Коммутируемые линии	низкая	низкая	низкая	низкая	низкая
Незащищенные потоки конфиденциальной информации	низкая	низкая	низкая	средняя	низкая
Неадекватное управление сетью	низкая	средняя	средняя	средняя	низкая
Незащищенные подключения к сетям общего пользования	низкая	низкая	низкая	низкая	низкая
5. Документы (документооборот)					

Хранение в незащищенных местах	низкая	средняя	средняя	низкая	низкая
Недостаточная внимательность при уничтожении	низкая	средняя	высокая	средняя	низкая
Бесконтрольное копирование	низкая	высокая	высокая	низкая	низкая
6.Персонал					
Отсутствие персонала	низкая	низкая	низкая	низкая	низкая
Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц	низкая	низкая	низкая	средняя	средняя
Недостаточная подготовка персонала по вопросам обеспечения безопасности	низкая	низкая	средняя	средняя	низкая
Отсутствие необходимых знаний по вопросам безопасности	низкая	средняя	средняя	средняя	низкая
Неправильное использование программно-аппаратного обеспечения	низкая	средняя	средняя	средняя	низкая
Отсутствие механизмов отслеживания	низкая	низкая	низкая	низкая	низкая
Отсутствие политики правильного пользования телекоммуникационными системами для обмена сообщениями	низкая	низкая	низкая	низкая	низкая
Несоответствующие процедуры набора кадров	низкая	низкая	низкая	средняя	низкая
7. Общие уязвимые места					
Отказ системы вследствие отказа одного из элементов	средняя	средняя	средняя	низкая	средняя
Неадекватные результаты проведения технического обслуживания	средняя	низкая	низкая	низкая	средняя

Приложение 4

Угрозы

Наименование возможных и вероятных угроз	Классы угроз
Землетрясение	С
Затопление	Б, А, С
Ураган	С
Попадание молнии	С
Забастовка	Б, А
Пожар	Б, А
Намеренное повреждение	Б
Неисправности в системе электроснабжения	А
Неисправности в системе водоснабжения	А
Неисправности в системе кондиционирования воздуха	Б, А
Аппаратные отказы	А
Колебания напряжения	А, С
Экстремальные величины температуры и влажности	Б, А, С
Воздействие пыли	С
Электромагнитное излучение	Б, А, С
Наименование возможных и вероятных угроз	Классы угроз
Статическое электричество	С
Кража	Б
Несанкционированное использование носителей данных	Б
Ухудшение состояния носителей данных	С
Ошибка обслуживающего персонала	Б, А
Ошибка при обслуживании	Б, А
Программные сбои	Б, А
Использование программного обеспечения несанкционированными пользователями	Б, А
Вредоносное программное обеспечение	Б, А
Незаконный импорт/экспорт программного обеспечения	Б
Ошибка операторов	Б, А
Ошибка при обслуживании	Б, А
Доступ несанкционированных пользователей к сети	Б
Технические неисправности сетевых компонентов	А
Ошибки передачи	А
Повреждение линий	Б, А
Несанкционированное проникновение к средствам связи	Б
Анализ трафика	Б
Направление сообщений по ошибочному адресу	А
Изменение маршрута направления сообщений	Б
Изменение смысла переданной информации	Б
Сбои в функционировании услуг связи (например, сетевых услуг)	Б, А
Недостаточная численность персонала	А
Ошибки пользователей	Б, А
Ненадлежащее использование ресурсов предприятия	Б, А

Приложение 5

Результаты оценки угроз активам

Группа угроз Содержание угроз	Сервера	БД	ПО	Документы	ПК
1. Угрозы, обусловленные преднамеренными действиями					
Затопление	никакая	никакая	никакая	никакая	никакая
Забастовка	никакая	никакая	никакая	никакая	никакая
Бомбовая атака	никакая	никакая	никакая	никакая	никакая
Применение оружия	никакая	никакая	никакая	никакая	никакая
Пожар	никакая	никакая	никакая	никакая	никакая
Намеренное повреждение	никакая	никакая	средняя	средняя	средняя
Неисправности в системе кондиционирования воздуха	никакая	никакая	никакая	никакая	никакая
Экстремальные величины температуры и влажности	никакая	никакая	никакая	никакая	никакая
Электромагнитное излучение	никакая	средняя	средняя	средняя	никакая
Кража	никакая	средняя	никакая	средняя	никакая
Несанкционированное использование носителей данных	никакая	средняя	никакая	никакая	никакая
Ошибка обслуживающего персонала	никакая	никакая	средняя	никакая	никакая
Ошибка при обслуживании	никакая	никакая	никакая	никакая	никакая
Программные сбои	никакая	средняя	никакая	никакая	никакая
Использование программного обеспечения несанкционированными пользователями	никакая	средняя	никакая	никакая	никакая
Использование программного обеспечения несанкционированным способом	никакая	средняя	никакая	никакая	никакая
Нелегальное проникновение злоумышленников под видом санкционированных пользователей	никакая	никакая	никакая	никакая	никакая

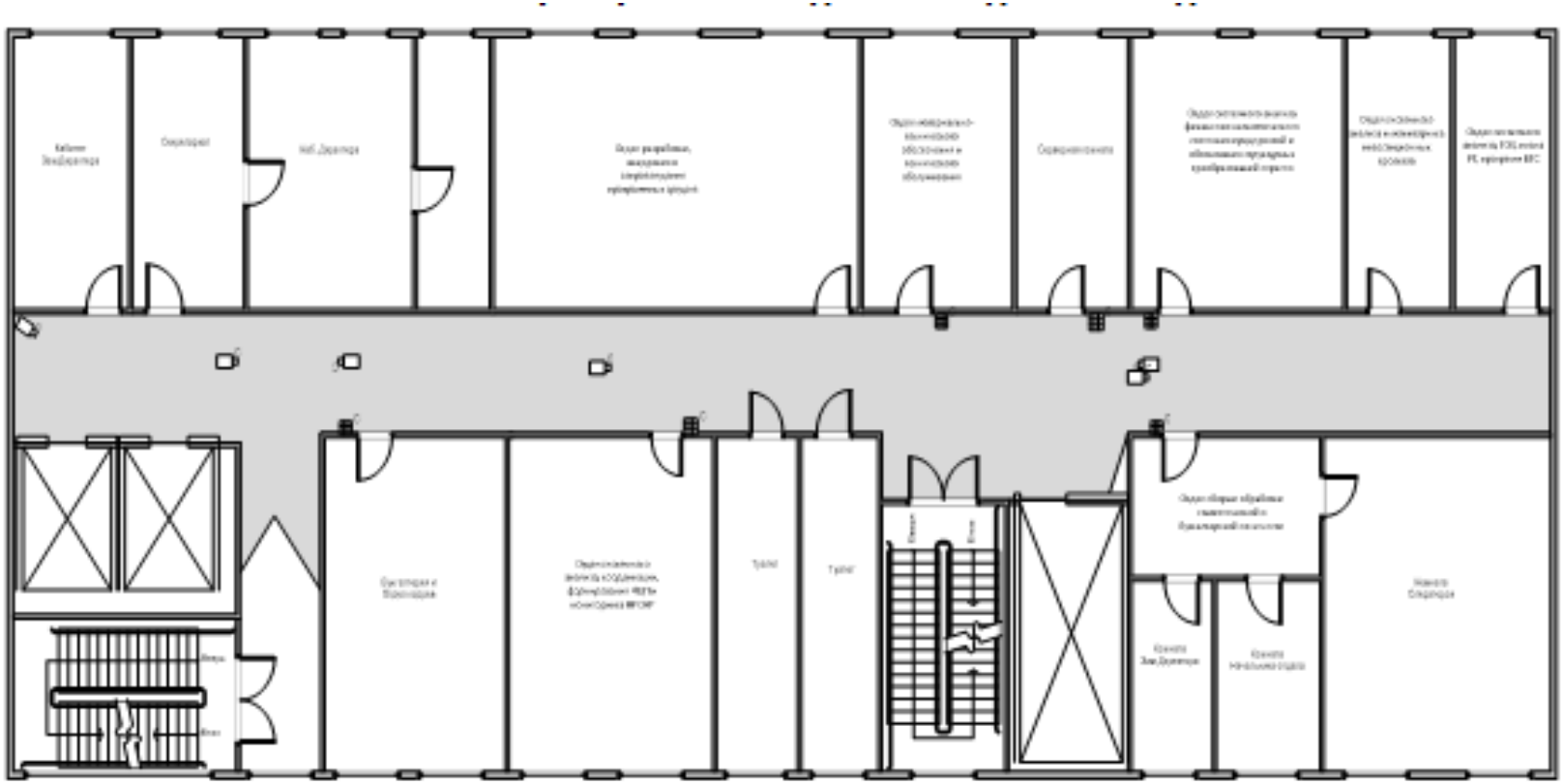
Незаконное использование программного обеспечения	низкая	низкая	низкая	низкая	низкая
Вредоносное программное обеспечение	низкая	низкая	низкая	низкая	низкая
Незаконный импорт/экспорт программного обеспечения	низкая	средняя	низкая	низкая	низкая
Ошибка операторов	низкая	низкая	высокая	высокая	низкая
Ошибка при обслуживании	низкая	низкая	низкая	низкая	низкая
Доступ несанкционированных пользователей к сети	низкая	низкая	низкая	средняя	низкая
Использование сетевых средств несанкционированным способом	низкая	низкая	низкая	низкая	низкая
Повреждение линий	средняя	низкая	низкая	средняя	низкая
Перегруженный трафик	средняя	высокая	средняя	высокая	низкая
Перехват информации	низкая	средняя	низкая	средняя	низкая
Несанкционированное проникновение к средствам связи	низкая	низкая	низкая	низкая	низкая
Анализ трафика	низкая	низкая	низкая	средний	низкая
Изменение маршрута направления сообщений	низкая	низкая	низкая	низкая	низкая
Изменение смысла переданной информации	низкая	низкая	средняя	средняя	низкая
Сбои в функционировании услуг связи (например сетевых услуг)	низкая	средняя	средняя	средняя	низкая
Ошибки пользователей	низкая	низкая	высокая	высокая	низкая
Ненадлежащее использование ресурсов	низкая	высокая	высокая	высокая	низкая
2. Угрозы, обусловленные случайными действиями					
Затопление	низкая	низкая	низкая	низкая	низкая
Забастовка	низкая	низкая	низкая	низкая	низкая
Бомбовая атака	низкая	низкая	низкая	низкая	низкая

Применение оружия	низкая	низкая	низкая	низкая	низкая
Пожар	низкая	низкая	низкая	низкая	низкая
Неисправности в системе электроснабжения	низкая	низкая	низкая	низкая	низкая
Неисправности в системе водоснабжения	низкая	низкая	низкая	низкая	низкая
Неисправности в системе кондиционирования воздуха	низкая	низкая	низкая	низкая	низкая
Аппаратные отказы	низкая	низкая	низкая	низкая	низкая
Колебания напряжения	низкая	средняя	средняя	средняя	низкая
Экстремальные величины температуры и влажности	низкая	низкая	низкая	низкая	низкая
Электромагнитное излучение	низкая	низкая	низкая	низкая	низкая
Ошибка обслуживающего персонала	низкая	низкая	средняя	низкая	низкая
Ошибка при обслуживании	низкая	низкая	средняя	низкая	низкая
Программные сбои	низкая	низкая	низкая	низкая	низкая
Использование программного обеспечения несанкционированными пользователями	низкая	низкая	низкая	низкая	низкая
Использование программного обеспечения несанкционированным способом	низкая	низкая	низкая	низкая	низкая
Незаконное использование программного обеспечения	низкая	низкая	низкая	низкая	низкая
Вредоносное программное обеспечение	низкая	низкая	низкая	низкая	низкая
Ошибка операторов	низкая	низкая	средняя	средняя	низкая
Ошибка при обслуживании	низкая	низкая	низкая	низкая	низкая
Технические неисправности сетевых компонентов	низкая	низкая	низкая	низкая	средняя
Ошибки передачи	низкая	низкая	низкая	средняя	низкая

Повреждение линий	низкая	низкая	низкая	низкая	низкая
Перегруженный трафик	средняя	средняя	низкая	низкая	низкая
Направление сообщений по ошибочному адресу	низкая	низкая	низкая	средняя	низкая
Сбои в функционировании услуг связи (например сетевых услуг)	низкая	низкая	низкая	низкая	низкая
Недостаточная численность персонала	низкая	низкая	низкая	низкая	низкая
Ошибки пользователей	низкая	низкая	средняя	средняя	низкая
Ненадлежащее использование ресурсов	низкая	низкая	низкая	низкая	низкая
3. Угрозы, обусловленные естественными причинами (природные, техногенные факторы)					
Землетрясение	низкая	низкая	низкая	низкая	низкая
Затопление	низкая	низкая	низкая	низкая	низкая
Ураган	низкая	низкая	низкая	низкая	низкая
Попадание молнии	низкая	низкая	низкая	низкая	низкая
Колебания напряжения	низкая	низкая	низкая	низкая	низкая
Экстремальные величины температуры и влажности	средняя	низкая	низкая	низкая	средняя
Воздействие пыли	средняя	низкая	низкая	низкая	средняя
Электромагнитное излучение	низкая	низкая	низкая	низкая	низкая
Статическое электричество	низкая	низкая	низкая	низкая	низкая
Ухудшение состояния носителей данных	средняя	низкая	низкая	низкая	средняя

Приложение 6

Расположение камер охранного видеонаблюдения на одном этаже



- охранная камера видеонаблюдения
- кодовый замок на двери
- область, охватываемая видеокамерами

Приложение 7

Обзор видеокамер

Наименование устройства	Стоимость /Оптом	Разрешение /чувствительность /фокусное расстояние	Прочее
Цветная купольная видеокамера AV Tech MC27	3280/26 20 руб.	600 ТВЛ. /0,05 Лк. /3.8 мм.	ИК-подсветка до 10 м. Матрица: H.R. Color CCD, 1/3 дюйма. Число эффективных пикселей (PAL): 752*582. Функция «день-ночь», AES, AGC, AWB, Видеосигнал: композитный, 1 В, 75 Ом.
Цветная купольная видеокамера AV Tech MC26	2840/22 70 руб.	600 ТВЛ. /0,1 Лк. /3.6 мм	ИК-подсветка до 15 м. Матрица: H.R. Color CCD, 1/3 дюйма. Число эффективных пикселей (PAL): 752*582. Функция «день-ночь», AES, AGC, AWB, BLC, Видеосигнал: композитный, 1 В, 75 Ом.
Цветная купольная видеокамера FE DV82A/15M	3230/29 50 руб.	470 ТВЛ. /0,02 Лк. /4 – 9 мм.	ИК-подсветка до 15 м. Матрица: Sony Super HAD II CCD, 1/3 дюйма. Число эффективных пикселей (PAL): 500*582. Функция «день-ночь», AES, AGC, AWB, BLC, Видеосигнал: композитный, 1 В, 75 Ом.
Цветная купольная видеокамера CNB LBM-21VF	5920/54 20 руб.	600 (ч/б:650)ТВЛ. /0,05 (ч/б:0,01)Лк. /3.8 – 9.5 мм	Динамическая ИК-подсветка до 15 м. Матрица: High Sensitivity CCD, 1/3 дюйма. Число эффективных пикселей (PAL): 752*582. Функция «день-ночь», AES, AGC, AWB, DNR, SBLC, Flickerless, Privacy Zone, Motion Detection, Mirror Function, OSD, Видеосигнал: композитный, 1 В, 75 Ом.

Приложение 8

Обзор видеорегистраторов

Цена (руб.)	Входы/выходы	Сетевые протоколы	Скорость записи (запись) /алгоритм сжатия (кодек) /качество записи
STR-1688 Цифровой видеорегистратор H.264; 16 каналов			
45794.18	Выходы мониторов: 1 BNC, 1 VGA Spot-вых: 4 BNC Аудио: 16/1 Тревожные: 16 TTL / 4 релейны + 12 TTL	TCP/IP; HTTP; DHCP	400 изобр./с (352x288 пикс.) 200 изобр./с (720x288 пикс.) 100 изобр./с (720x576 пикс.) / H.264 / 4 уровня: Very High/High/Standard/Low
Прочее: Тип/количество HDD: 1 встроенный SATA HDD (в комплекте), установка 2 дополнительных HDD; Форматы отображения: 1, 4, 9, 13, 16 окон; Режимы воспроизведения: Перемотка вперед/назад (x2, x4, x8, x16, x32), покадровый просмотр, пауза, обратное воспроизведение;			
DVR1604LE-AS 16-ти канальный цифровой видеорегистратор. Пентаплекс.			
11400	Выходы мониторов: 1 TV, BNC, 1 VGA; Аудио: 4/1; Тревожные вх.: 16; Релейные вых.: 3 канала, 30VDC, 1A, NO/NC	TCP/IP; DHCP; Email; UDP; DNS; FTP; IP Filter; PPPOE; DDNS; Alarm Server	D1/4CIF(704*576/704*480) - 6 кад/сек (25 кад/сек - первый и девятый канал); 2CIF(704*288/704*240) , CIF(352*288/352*240) , QCIF(176*144/176*120) - 25 кад/сек /H.264 /6 выбираемых уровня (6 наивысший)
Прочее: Жесткий диск HDD: 1 x 3.5" SATA (объемом до 2 ТБ); Форматы отображения: 1, 4, 8, 9, 16 окон; Режимы воспроизведения: одновременно четыре канала, воспроизведение, пауза, стоп, быстрый просмотр, медленный просмотр, следующий файл, предыдущий файл, следующая камера, предыдущая камера, полноэкранный режим, повтор, выборочное резервное копирование			
Ai-D365 16-канальный регистратор в корпусе из сплава алюминия			

14435	Видео: 16 BNC/ 2 BNC, 1 D-Sub VGA Аудио: 2/1;	TCP/IP; HTTP; PPPoE; DHCP; FTP; DDNS; TSM	60 кадр/сек. (720x480), 120 кадр/сек. (720x240), 240 кадр/сек. (360x240) (NTSC); 50 кадр/сек. (720x576), 100 кадр/сек. (720x288), 200 кадр/сек. (360x288) (PAL) /H.264
Прочее: Поддержка жёстких дисков: Поддержка одного жесткого диска типа 3,5» SATA до 2 Тб каждый и более; Режим записи: Ручной режим/постоянная/ по расписанию/ по тревоге; Режим воспроизведения: По кадрам. Ускоренное воспроизведение вперед и назад (до 64х); Функции тревоги: 1. Детекция движения (с конфигурируемой областью и чувствительностью) 2. Потеря изображения 3. Вход датчика 4. 8 контактов на датчики или сигнал TTL/CMOS, выбираемая полярность 5. Отправка e-mail сообщения на стационар			
DVR3116. 16-ти канальный цифровой видеорегистратор.			
8900	Видео: 16 BNC/ 1 TV BNC, 1 VGA Аудио: 4/1	TCP/IP; UDP; DHCP; DNS; IP Filter; PPPoE; DDNS; FTP; Email; Alarm Server	(D1 - 704x576; CIF - 352x288) 6 кад/с (D1) 25 кад/с (CIF) /H.264
Прочее: Жесткий диск: 1 порт SATA, максимальный объем жесткого диска 2TB; Форматы отображения: 1, 4, 8, 9, 16 окон; Режим записи: Вручную, По расписанию (Постоянная, По детекции (видео детекция: определение движения, пустой экран, потеря видеосигнала), Тревога), Стоп; Приоритет записи: Ручная > Тревога > Детекция движения > Постоянная; Функции воспроизведения: Воспроизведение, пауза, стоп, быстрый просмотр, медленный просмотр, следующий файл, предыдущий файл, следующая камера, предыдущая камера, полноэкранный режим, повтор, выборочное резервное копирование, изменение масштаба изображения до любого размера.			

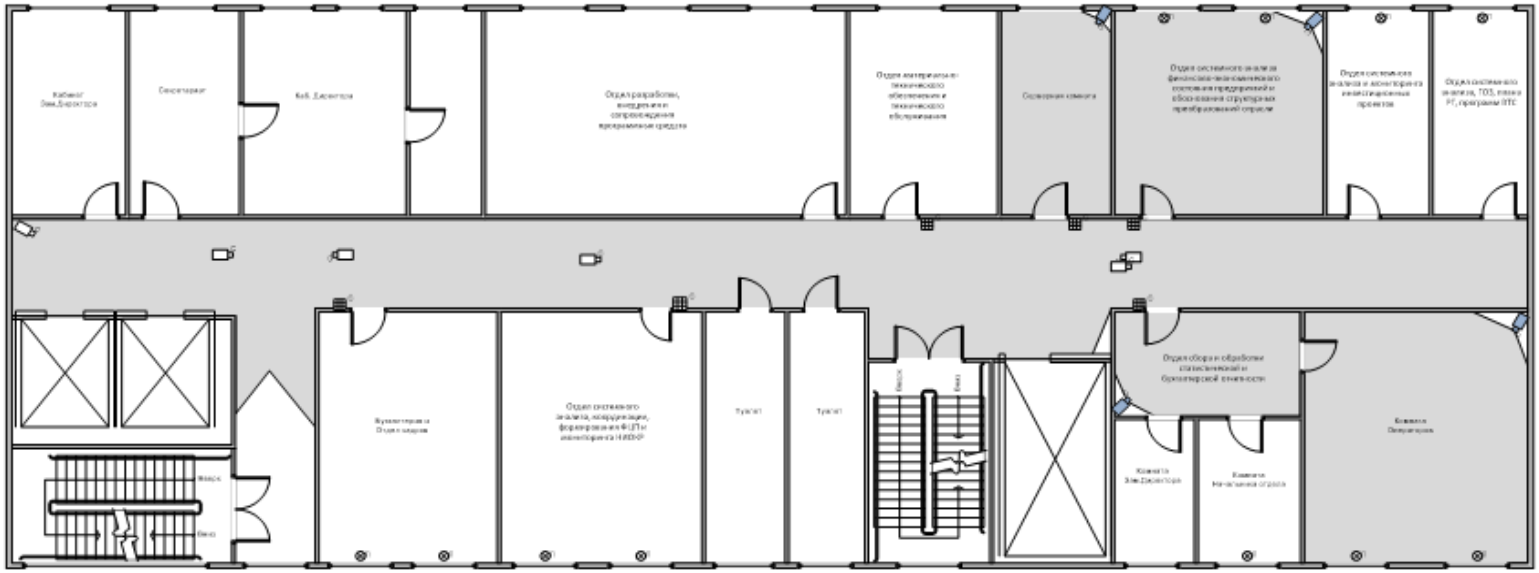
Приложение 9

Обзор генераторов шума

Наименование	Цена (руб.)	Диапазон частот	Прочее
«Гром-ЗИ-4Б», система защиты информации	11000	Первый канал: 0,01 – 30 МГц Второй канал: 0,01 – 2000 МГц	Система состоит из генератора шумовой помехи «Гром-ЗИ-4Б», дисконусной антенны «SI-5002.1» и трёх рамочных антенн. Система защиты «Гром-ЗИ-4Б» предназначена для маскировки побочных электромагнитных излучений и наводок (ПЭМИН) средств вычислительной техники.
пространственное зашумление НЭТ «Штора-4»	83570	0,1 – 2500 МГц	Конструктивно генератор выполнен в металлическом корпусе, камуфлированном в сумке для работы в автономных условиях.
пространственное зашумление SEL SEL SP-21 «Баррикада»	11185	0,1 - 2000 МГц	Область использования – помещения, в которых расположены средства вычислительной техники с информацией от конфиденциальной до содержащей сведения, составляющие государственную тайну.

Приложение 10

Расположение видеокамер и генераторов шума



- охранная камера видеонаблюдения

- камера видеонаблюдения предприятия «Хендай» ГК «Вектор»

- генератор шума системы «Гром-ЗИ-4Б»

- кодовый замок на двери

- область, охватываемая видеокамерами

Приложение 11

Таблица 9

Анализ выполнения основных задач по обеспечению информационной безопасности

Основные задачи по обеспечению информационной безопасности	Степень выполнения
обеспечение безопасности производственно-торговой деятельности, защита информации и сведений, являющихся коммерческой тайной;	средняя
организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;	высокая
организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;	высокая
предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну;	средняя
выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (авария, пожар и др.) ситуациях;	высокая
обеспечение режима безопасности при осуществлении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с деловым сотрудничеством на национальном и международном уровне;	средняя
обеспечение охраны территории, зданий помещений, с защищаемой информацией.	средняя

Приложение 12

Таблица 10

Оценка в денежных единицах

Название уровня	Оценка уровня, у.е.
Низкий	до 100 тыс.
Средний	от 100 тыс. до 3 млн.
Высокий	свыше 3 млн.

Принципы оценки критичности каждого указанного актива:

Приложение 13

Таблица 12

Содержание и объем разового ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п\ п	**Выполняемые действия**	**Среднечасовая зарплата специалиста (руб.)**	**Трудоемкость операции (чел. час)**	**Стоимость, всего (руб.)**
1	Закупка утвержденных начальником отдела безопасности и руководством ПиАСИБ	300	8	2 400
2	Монтаж и установка аппаратных и программных СЗИ	200	24	4 800
3	Настройка и отладка установленных средств ИБ	300	8	2 400
4	Проведение занятий по обучению и использованию данных СЗИ с сотрудниками отдела	350	4	1 400
5	Контроль и мониторинг работоспособности системы защиты информации	150	88	13 200
Стоимость проведения организационных мероприятий, всего				24 200
Мероприятия инженерно-технической защиты				
№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (руб.)	Кол-во (ед.измерения)	Стоимость, всего (руб.)
1	Цветная купольная видеокамера AV Tech MC27	2620	6	15 720
2	Ai-D365 16-канальный регистратор в корпусе из сплава алюминия	14 435	1	14 435
3	«Гром-ЗИ-4Б», система защиты информации	11 000	4	44 000
Стоимость проведения мероприятий инженерно-технической защиты				74 155
Объем разового ресурса, выделяемого на защиту информации				98 355

Приложение 14

Таблица 13

Содержание и объем постоянного ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п\п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел. час)	Стоимость, всего (руб.)
1	Выполнение плановых мероприятий администратора ИБ (сотрудника отдела безопасности)	200	88	17 600
2	Физическая охрана помещений, где установлены СЗИ	200	22	3 400
3	Своевременное обслуживания программных и аппаратных средств защиты информации	350	4	1 400
Стоимость проведения организационных мероприятий, всего				22 400
Мероприятия инженерно-технической защиты				
№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (руб.)	Кол-во (ед.измерения)	Стоимость, всего (руб.)
1	Цветная купольная видеокамера AV Tech MC27	2620	2	5 240
2	«Гром-ЗИ-4Б», система защиты информации	11 000	1	11 000
Стоимость проведения мероприятий инженерно-технической защиты				16 240
Объем постоянного ресурса, выделяемого на защиту информации				38 640

Приложение 14

Таблица 14

Величины потерь (рисков) для критичных информационных ресурсов после внедрения/модернизации системы защиты информации

Актив	Угроза	Величина потерь (руб.)
Сервера	Кража, повреждения	50 000
БД	Несанкционированный доступ (кража)	5 000
ПО	Несанкционированный доступ (кража)	1 000
Документы	Кража, повреждения	1 000
Пользовательские компьютеры	Кража, повреждения	1 000
Суммарная величина потерь		58 000

Приложение 15

Таблица 15

Оценка динамики величин потерь

	1 кв.	2 кв.	3 кв.	1 год
До внедрения СЗИ	57 500	115 000	172 500	230 000
После внедрения СЗИ	14 500	29 000	43 500	58 000
Снижение потерь	43 000	86 000	129 000	172 000

Приложение 16

Результаты ранжирования конфиденциальной информации

Наименование информации	Ценность (ранг)
Обработка документов	1
Обеспечение непрерывной работы	2
Обмен корреспонденцией	2
Защита данных	3
Управление данными	3
Обработка документов	3
Доступ к информационным ресурсам	3
Пользовательские компьютеры	4
Документы	4
Разработка программного обеспечения по конкурсам	5
Сервера	5
Доступ к информационным ресурсам	5

Приложение 17

Таблица 2

Классификация мотивации внутренних нарушителей[24]

Класс мотивов	Содержание и характеристика
Личные мотивы сотрудника	личные финансовые трудности, невозможность удовлетворения жизненных потребностей своих и семьи;
	психологическая готовность (предрасположенность) работника к злоупотреблению служебным положением;
	порочные связи, поступки, увлечения;
	несоответствие квалификации сотрудника занимаемой должности
Внутренние мотивы организации	наличие слабых мест в системе управления деятельностью фирмы (в частности, в системе управленческого учета);
	низкая квалификация руководства организации;
	нездоровый деловой климат в коллективе организации;
	слабый кадровый менеджмент, который позволяет занимать ответственные должности сотрудникам-аферистам, неэффективная персональная работа с кадрами;
	отсутствие или слабость корпоративной политики и этики;
	слабая организация системы обучения персонала;
	неэффективная система мотивации (нет анализа потребностей каждой личности и персональной мотивации);
	некачественная проверка кандидатов при приеме на работу
Внешние мотивы	условия материальной и/или моральной мотивации у конкурентов лучше;
	установка конкурентов на переманивание;
	внешнее давление на сотрудников;
	втягивание их в разные виды зависимости;
	инфляционные процессы (их следует учитывать при расчете заработной платы)

Приложение 18

Результаты оценки рисков информационным активам организации

Риск	Актив	Ранг риска
Кража	Сервера	6
Несанкционированный доступ	БД	6
Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц	БД	6
Сбои / ошибки	БД	6
Несанкционированный доступ	Сервера	5
Сбои / ошибки	Сервера	5
Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц	БД	5
Сбои / ошибки	ПО	5
Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц	Документы	5
Кража	ПК	5
Несанкционированный доступ	ПК	5
Сбои / ошибки	ПК	5
Несанкционированный доступ	ПО	4
Несанкционированный доступ	Документы	4
Сбои / ошибки	Документы	4

Приложение 19

Рекомендуемые мероприятия с целью минимизации риска утечки конфиденциальной информации на бумажных носителях в ООО «Вектор»

№	Описание мероприятия
1	формирование правовых условий защиты конфиденциальной информации, непосредственно в компании, путем разработки нормативно-правовых документов по защите всех видов информации (документированной, электронной, а также информации, существует в виде знаний работников ООО «Вектор»), которыми должны регулироваться взаимоотношения компании с его сотрудниками, клиентами и т.д.;
2	обеспечение контроля за бумажными носителями конфиденциальной информации, в первую очередь сотрудниками ООО «Вектор», в части соблюдения работниками установленного режима защиты информации, своевременное реагирование на все нарушения в защите информации;
3	повышение прозрачности отчетности и ужесточение требований к обеспечению достоверности информации, также проведение внешнего и внутреннего аудита ООО «Вектор».
4	повышение квалификации сотрудников ООО «Вектор» в области экономической и информационной безопасности;
5	обеспечение надежной охраны организации ООО «Вектор» для исключения возможности несанкционированного доступа к информации, выноса документов;
6	внедрение надежной системы документооборота (служебного и специального делопроизводства), который исключает возможность несанкционированного доступа к документам, их потери, уничтожения или модификации