МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Организация обеспечения информационной безопасности в гостиничной индустрии на примере отеля «Nevsky Contour»

Исполнитель Рябова Екатерина Евгеньевна
(фамилия,имя,отчество)

Руководитель доктор технических наук, профессор
(ученая степень, ученое звание)

Бескид Павел Павлович
(фамилия, имя, отчество)

«К защите допускаю»

Заведующи йкафедрой

(подпись)

доктор технических наук, профессор
(ученаястепень,ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия,имя,отчество)

«17» февраля 2017 г.

Санкт–Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Организация обеспечения информационной безопасности в гостиничной индустрии на примере отеля «Nevsky Contour»

Исполнитель Рябова Екатерина Евгеньевна
(фамилия,имя,отчество)

Руководитель доктор технических наук, профессор
(ученая степень, ученое звание)

Бескид Павел Павлович
(фамилия, имя, отчество)

«К защите допускаю»

Заведующи йкафедрой

_____
(подпись)

доктор технических наук, профессор
(ученаястепень,ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия,имя,отчество)

«__»_____20__г.

Санкт–Петербург

2017

РЕФЕРАТ

Отчет 99 с., 4 ч., 13 рис., 13 табл., 32 источников, 2 прил.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ, КОММЕРЧЕСКАЯ ТАЙНА, УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ТЕХНИЧЕСКАЯ И ПРОГРАММНАЯ ЗАЩИТА ИНФОРМАЦИИ, ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ.

Объектом исследования является техническое, программное и организационное обеспечение отеля «Nevsky Contour», а также комплекс мер по защите этого обеспечения.

Цель дипломного проекта - разработать комплекс мер по обеспечению информационной безопасности отеля «Nevsky Contour». Оценить и доказать эффективность созданной системы информационной безопасности.

Задачи, которые необходимо решить в работе для достижения цели :

- анализ деятельности отеля «Nevsky Contour»;
- обосновать угрозы безопасности информации;
- оценка состояния существующей защищенности отеля «Nevsky Contour»;
- разработать комплекс мер по обеспечению информационной безопасности в отеле «Nevsky Contour»;
- оценка эффективности разработанной системы безопасности.

В работе разработаны и представлены:

- порядок анализа состояния защищенности информации в коммерческой организации;
- предложение комплекса мер по обеспечению информационной безопасности;
- обоснование экономической составляющей и эффективности разработанной системы обеспечения безопасности информации.

Оглавление

Введение

Проблема безопасности занимает в современном мире одну из самых серьезных позиций, являясь глобальной проблемой современности. Безопасность можно рассматривать в разных сферах жизнедеятельности человека, но, как бы то ни было, в любой сфере, где человек вступает в контакт с природой, техникой или другим человеком и группой людей, возникают определенные риски. Современные компьютерные технологии активно внедряются в сферу социально-культурного сервиса и туристского бизнеса, их применение становится неотъемлемым условием успешной работы. Сами по себе гостиницы — это сложный механизм, поэтому обеспечить безопасность информации в них непросто. Известное изречение «Кто владеет информацией, тот владеет миром» особенно актуально для сферы туристского бизнеса, так как именно оперативность, надежность, точность, высокая скорость обработки и передачи информации во многом определяют эффективность управленческих решений в этой области. Любые управленческие информационные процессы включают в себя процедуры регистрации, сбора, передачи, хранения, обработки, выдачи информации. Ежедневно через заведения проходит масса людей, которые потенциально обладают какими-то ценностями. Все данные отражаются в базе гостиницы, то есть теоретически есть такое место, откуда эти данные можно «вытащить». Именно эти действия непрерывно связаны с опасностью и возникновением рисков, к которым можно отнести утечку конфиденциальной информации и несанкционированный доступ к информационным ресурсам.

О безопасности здесь заботятся двадцать четыре часа в сутки, и насколько эффективны современные методы зависит от, организации структуры службы безопасности, финансирования, технического обеспечения безопасности, квалифицированности персонала и т.п.

Актуальность дипломной работы подтверждается тем фактом, что в последнее десятилетие туризм превратился в заметную составляющую экономики России, следовательно, чем более весомую роль начинает играть отрасль в эко-

номике государства, тем большее количество людей вовлекается в ее функционирование и тем более усиленное внимание необходимо уделять вопросам обеспечения безопасности в этой отрасли.

На сегодняшний день в ООО «Ат-Сервис» отсутствует грамотно организованная система информационной безопасности, не смотря на то, что в Обществе ежедневно циркулирует и обрабатывается информация, которая согласно федеральному закону «О коммерческой тайне» закрыта от свободного распространения.

Основными факторами, определяющими актуальность проблемы, является:

– обострение противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование

– повышение уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности

– вовлечение в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса

– концентрация больших объемов информации различного назначения и принадлежности на электронных носителях

– количественное и качественное совершенствование способов доступа пользователей к информационным ресурсам

– отношение к информации, как к товару, переходом к рыночным отношениям в области предоставления информационных услуг с присущей им конкуренцией и промышленным шпионажем

– многообразие видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации

– рост числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации

– увеличение потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов).

Объектом дипломного проекта выступает общество с ограниченной ответственностью «Ат-Сервис», которое выполняет функции по приему и размещению постояльцев в отеле «Nevsky Contour».

Предметом дипломного проекта выступает система обеспечения информационной безопасности средств хранения, обработки и передачи данных в ООО «Ат-Сервис».

Целью дипломного проекта является разработка комплекса мер по обеспечению информационной безопасности в отеле «Nevsky Contour» .

Для достижения данной цели необходимо решить ряд задач:

- Выявить угрозы безопасности и каналы утечки информации на объекте исследования;
- Разработать комплекс мер по обеспечению защиты данных от выявленных каналов утечки информации;
- Аргументировать и подкрепить доводами выбранный состав средст защиты информации;
- Оценить практическую пользу, эффективность и экономическую составляющую по защите информации;

Структурно работа состоит из введения, трех глав, заключения и списка использованных источников.

Первая глава посвящена анализу обеспечения информационной безопасности в коммерческой организации.

Во второй главе проводится анализ состояния системы информационной безопасности отеля «Nevsky Contour».

Третья глава посвящена проектированию системы информационной

безопасности отеля «Nevsky Contour».

Для анализа существующей системы безопасности отеля «Nevsky Contour» в работе будут использованы практические и аналитические материалы.

1 Анализ обеспечения информационной безопасности информации

1.1Актуальность и значимость обеспечения информационной безопасности

В век технологий такой вопрос, как информационная безопасность должен решаться с большим пониманием. Особенно если речь идет о заведениях, где есть интенсивная работа с клиентами и их личными данными. Именно такими заведениями и являются гостиницы.

Информационная безопасность гостиницы, либо любого другого коммерческого предприятия, выражается уровнем защиты данных, благодаря которому мошенникам крайне трудно или невозможно завладеть важной для клиента или самого заведения информацией. Каждый день клиенты гостиниц производят оплаты посредством пластиковых карт, а так же оставляют в базе паспортные и личные данные. Все это должно быть доступно исключительно для нужд гостиницы до тех пор, пока клиент не покинет заведение. Все данные, так или иначе, связаны с финансовыми операциями, поэтому их нужно тщательно скрыть. В периоды, когда информационная безопасность не занимала высокий уровень, в крупных гостиницах мошенники практиковали очень хитрую схему: они доставали данные о счетах постояльцев, и каждый день снимали сразу с нескольких счетов незначительную сумму. Это могло быть 10 долларов, поэтому пропажу денег клиент замечал не сразу, а только после накопления серьезной суммы. Чтобы подобных ситуаций не происходило, следует как раз обеспечивать высокий уровень безопасности.

Обеспечение безопасности посетителей, в том числе информационной — это одна из главных задач владельца и персонала гостиницы. Только так можно говорить о том, что заведение будет пользоваться популярностью у людей. Без доверия в этой сфере очень быстро можно потерять даже самый высокий рейтинг, вот почему на современной технике и на ее обслуживании сейчас экономить не принято[10].

В конкурентных условиях рынка, информация может покупаться и про-

даваться и быть одним из самых ценных товаров. Из этого следует, что информацию, как и любой другой продукт, следует оберегать и защищать.

Развитие и распространение информационных технологий не стоит на месте, что превращает информационную безопасность в более сложный и дорогостоящий процесс. В некоторой мере эта связь отражается в компромиссе большинства современных организаций: осуществление открытой рекламы предоставляемых товаров и услуг, и при этом выполнять защиту своих интересов, обеспечивая безопасность конфиденциальной информации любыми законными способами.

Проблема защиты информации возникает там, где есть противоречия, конфликт интересов в информационной среде. Исходя из этого, можно сделать вывод, что защита информации представляет собой многогранную проблему, часть которой еще даже не имеет четких границ. Наиболее разработаны вопросы защиты информации, содержащей государственную, коммерческую и прочие тайны [3].

Очень часто защиту информации классифицируют на:

– Организационно-правовую;
– Программно-аппаратную;
– Инженерно-техническую.

Понятие организационно-правовой защиты тесно связано с выполнением регламентов нормативно-правовой документации.

В свою очередь программно - аппаратное обеспечение безопасности информации реализует задачи защиты вычислительных систем и средств путем предотвращения несанкционированного доступа, а так же использованием криптографической защиты данных.

Инженерно-техническая защита информации выполняет функции обеспечения безопасности информации с использованием инженерных конструкций и специальных программных средств.

Именно последний тип защиты приобретает все большее значение. Объясняется это следующими факторами:

– Развитие технических средств и методов обработки информации позволяет получить несанкционированный доступ к конфиденциальной информации на безопасном расстоянии от объекта исследования;

– Относительно простой доступ к рынку современной микроэлектроники , позволяющий за относительно не большие деньги приобрести компактные и скрытные технические средства для получения несанкционированного доступа к конфиденциальной информации на расстоянии;

– Оснащение служебных зданий повседневной электро- и радиоаппаратурой, в которой могут протекать неконтролируемые физические процессы, съем которых позволяет получить доступ к конфиденциальной информации. [1].

Оценивая все вышеперечисленные доводы можно сказать, что грамотное и полное обеспечение защиты информации может быть организовано при комплексном применении современных технических и программных средств.

Под угрозами информационной безопасности следует понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию. Такие угрозы, воздействуя на ресурсы, могут привести к искажению данных, копированию, несанкционированному распространения, ограничению или блокированию к ним доступа. Угрозы бывают умышленные и случайные.

Случайные угрозы, или по-другому непреднамеренные угрозы это такие угрозы, которые не связаны с действиями злоумышленников, к примеру: ошибки оператора, аварии, аппаратные и программные неисправности технических средств, неосознанные или не корректные действия технического персонала, случайные непреодолимые силы, пожары, наводнения и другие стихийные бедствия. Механизм их реализации изучен достаточно хорошо, поэтому существуют разработанные методы противодействия.

К умышленным или преднамеренным угрозам относят целенаправленные действия злоумышленника, таким как: хищение, модификация, уничтожение данных и т.д. Данный класс имеет динамический характер и постоянно попол-

няется новыми видами угроз. Преступные действия злоумышленника будут направлены на следующие технические каналы утечки информации:

- Оптические;
- Радиоэлектронные;
- Акустические;
- Электромагнитные;
- Материально-вещественные.

Информационным носителем в оптическом канале будет считаться электромагнитное поле (элементарными частицами являются фотоны) в диапазоне видимого света 0,45-0,75 мкм и диапазоне инфракрасного излучения 0,75-14 мкм.

В радиоэлектронном канале утечка данных происходит через электрические, магнитные и электромагнитные сигналы в радиодиапазоне, а так же электрический ток.

Акустический канал утеки информации характеризуется неконтролируемым распространением акустических сигналов в инфразвуковом диапазоне (до 16Гц), звуковом (16-20Гц) и ультразвуковом диапазоне (более 20кГц)[11].

Основными источниками утечки информации в материально вещественном диапазоне являются субъекты(люди) и материальные объекты такие как: документы, черновики, компакт-диски и другие устройства хранения. Компрометация конфиденциальной информации в таком случае может произойти в результате неправильного взаимодействия субъектов и материальных объектов. Например, в результате неконтролируемой утилизации отходов делопроизводства. Именно таким образом, документы содержащие в себе коммерческую тайну, могут попасть к злоумышленнику, который может попытаться продать их заинтересованным конкурентным организациям.

Каждый из приведенных выше каналов утечки информации обладает своими уникальными свойствами, которые необходимо учитывать при планировании политики информационной безопасности на предприятии.

Как правило, обычный канал утечки информации состоит из передатчика,

среды распространения и приемника - такая система является одноканальной.

Однако на практике очень часто встречаются более сложные системы, состоящие из 2х и более каналов утечки информации, поэтому их называют составными. Например, если в защищаемом объекте ведется разговор, то несанкционированный доступ к нему можно осуществить тремя способами: съемом звуковых волн через окна, двери, стены (акустический канал), наводкой лазерного луча на окна (оптический канал) и с помощью радиозакладки (радиоэлектронный канал).

Каналы утечки информации можно классифицировать по способу создания на умышленно организованные и случайные. Специально организованные каналы утечки создаются злоумышленниками для регулярного съема данных. Например, для получения несанкционированного доступа на удаленном расстоянии, на объекте можно разместить радиопередающее диктофонное устройство. Соответственно, злоумышленнику будут известны физические свойства данной радиозакладки, поэтому используя приемник с заранее известными характеристиками (частота, модуляция и мощность сигнала) появляется возможность регулярного доступа к конфиденциальной информации.

Побочные электромагнитные излучения и наводки могут стать причиной для создания случайного канала утечки информации. Злоумышленнику заранее не известны физические свойства таких излучений, но в случае правильного анализа частоты побочного излучения, то в нем можно выделить информативную составляющую, что и будет случайным каналом утечки информации. При некоторых условиях (время работы, мощность сигнала) такой канал может предоставить достаточно много полезной информации[1].

1.2 Анализ применения современных методов и средств по защите информации

Понятие коммерческой тайны возникло вместе с коммерческими организациями и является неотъемлемой частью отношений в странах, где наряду с

государственной существуют и другие формы собственности. Сущность коммерческого шпионажа- это стремление к овладению секретами конкурентов всеми доступными методами (включая применение специальных технических средств и подкуп должностных лиц) с целью получения максимальной выгоды.

При коммерческом шпионаже интересы государства остаются в стороне от прямого негативного воздействия, шпионаж все же остается не законным видом деятельности, так как покушается на конституционные права граждан. Государство стоит на защите прав граждан, а значит, что нарушение ведет к уголовной ответственности.

Для решения задач защиты информации от коммерческого шпионажа, в любой организации создается система защиты информации (СЗИ) [2].

СЗИ представляет собой комплекс мер, обеспечивающих заданную эффективность защиты информации организации.

Основными задачами системы защиты информации является создание условий для непрерывного и устойчивого развития коммерческой организации, а так же обнаружение и предотвращение посягательств на его безопасность.

СЗИ обеспечивает:

– защиту прав и коммерческих интересов организации;

– безопасность персонала;

– защиту материально-технических и финансовых ресурсов;

– ограничение и разграничение доступа к информационным и техническим ресурсам организации.

– Ориентируясь на задачи системы защиты информации, можно отметить три важнейших этапа создания СЗИ:

– Методологический- включает в себя создание нормативно-методологической документации, в которой раскрываются вопросы правил разработки и поддержки СЗИ;

– Организационный - обеспечивает создание организационно-распорядительной документации, а также на данном этапе производится обучение и инструктаж сотрудников;

– Технический - подбор, закупка и установка программно-аппаратных средств и каналов коммуникации.

Под методологическими основами комплексной защиты информации (как и решения любой другой проблемы) понимается совокупность принципов, подходов и методов (научно-технических направлений) необходимых и достаточных для анализа (изучения, исследования) проблемы комплексной защиты, построения оптимальных механизмов защиты и управления в процессе их функционирования. Уже из приведенного определения следует, что основными компонентами научно-методологических основ являются принципы, подходы и методы. При этом под принципами понимается основное исходное положение какой-либо теории, учения, науки, мировоззрения; под подходом - совокупность приемов, способов изучения и разработки какой-либо проблемы;; под методом - способ достижения какой-либо цели, решения конкретной задачи. Например, при реализации принципа разграничения доступа в качестве подхода можно выбрать моделирование, а в качестве метода реализации - построение матрицы доступа.

Общее назначение методологического базиса:

– Формирование обобщенного взгляда на организацию и управление СЗИ, отражающего наиболее существенные аспекты проблемы;

– Формирование полной схемы принципов, следование которым обеспечивает наиболее полное решение основных задач;

– Формирование совокупности методов, необходимых и достаточных для решения всей совокупности задач управления.

Основным элементом организационного этапа являются люди, условно разбиваемые на исполнителей и организаторов. Функциями организаторов являются контроль и управление над исполнением, а исполнителей – физическое воздействие на объекты труда. Множество исполнителей и их орудиями труда образуют объект управления (ОУ), множество организаторов вместе с информацией, техникой, специалистами и обслуживающим персоналом – субъект управления (СУ).

Невозможно провести четкую границу между СУ и ОУ, поскольку управленческая деятельность бессмысленна без исполнительной, а последняя немыслима без управленческой. Однако такое разделение является полезным для построения организационных систем.

Понятие ОС тесно связано с понятием «деятельность», так как основной задачей ОС является координация и осуществление деятельности людей, направленной на решение проблем. В связи с этим деятельность можно определить как осознанное и направленное на решение проблемы поведение людей[2].

Технический этап создания системы защиты информации включает в себя комплекс мероприятий по обеспечению защиты информации, предусматривающий использование программно-аппаратных средств, а также организационно технических решений различной сложности.

Организация работы по обеспечению технической безопасности основывается на исключении каналов утечки данных путем подавления наведенных информационных сигналов или снижения показателей сигнал/шум до наиболее приемлемых величин, обеспечивающих заданный уровень информационной безопасности.

Технические мероприятия по обеспечению информационной безопасности можно классифицировать на пассивные и активные.

Классификация технических средств представлена на рисунке 1.1.

Рисунок 1.1- Классификация технических средств.

Поиск и деактивация компактных электронных закладных устройств, предназначенных для перехвата информации, осуществляется выполнением исследований служебных помещений, с помощью специального оборудования. При этом осуществляется:

– Обнаружение закладок с использованием пассивного оборудования;

– Размещение в служебных кабинетах специальных устройств – обнаружителей диктофонов;

– Поиск аппаратных закладок при помощи индикаторов поля и программно-аппаратных комплексов контроля;

– Обнаружение закладок с использованием активного оборудования;

– Анализ служебных помещений с использованием нелинейных локаторов;

– Проверка служебных помещений, и аппаратно-программных средств с использованием рентгеновских комплексов [2].

1.3 Обзор правовой документации в области защиты информации.

В любой туристической организации разработка и внедрение системы обеспечения информации должно строго соответствовать всем нормативно-правовым документам в этой области и не нарушать законодательства на международном и государственно-отраслевом уровне, в частности законодательства Российской Федерации.

Информационная безопасность в сфере туризма на межгосударственном уровне осуществляется путем формирования и реализации международной политики по обеспечению безопасности и снижению рисков утечки информации. Такая политика формируется на представительных международных межправительственных или межпарламентских совещаниях, проводимых под эгидой Всемирной туристской организации.

На данном уровне субъектом управления является межправительственная Всемирная туристская организация (ВТО), созданная в 1994г и ведущая управляющие воздействия в виде деклараций, конференций и информационных сообщений через соответствующие печатные издания.

Первым документом ВТО, в котором нашли свое отражение вопросы безопасности и информационной безопасности в туризме, стала Хартия туризма. В статье III говорится о том, что государствам в интересах настоящих и будущих поколений следует защищать туристскую среду, обеспечивать безопасность посетителей, их имущества и конфиденциальных данных, а так же усиливать уже существующие меры защиты.

В декларации Гаагской Межпарламентской конференции по туризму (1989 г.) отмечалось, «что безопасность (социальная, информационная, экологическая и т.д.), защита туристов и уважение их достоинства является непременным условием развития туризма». В декларации даны развернутые рекомендации государствам и частному сектору по обеспечению условий безопас-

ности. Государства должны:

– сотрудничать при подготовке программ обеспечения безопасности;

– информировать общественность о возможных угрозах;

– формировать эффективную государственную политику, направленную на обеспечение социальной и информационной безопасности туристов;

– выполнять в каждой отдельной стране юридические положения в области защиты туристов, включая правоспособность туристов добиваться эффективной судебной защиты в судах в случае действий, наносящих любого вида ущерб;

– следить за выполнением законов и постановлений в стране и регионе всеми ведомствами и министерствами, так или иначе связанными с обслуживанием туристов;

– обеспечить энергичный подход к вопросу об информационной безопасности в туризме на глобальной и систематической основе[12].

Информационная безопасность на государственно-отраслевом уровне осуществляется путем формирования и реализации государственной политики и государственной программы по безопасности туризма, а также формирования соответствующей законодательной базы. На данном уровне субъектом управления является парламент, правительство страны основными задачами которых является соблюдение рекомендаций Гаагской конференции при помощи нормативно-правовых документов государственного законодательства.

В перечень основополагающих документов по защите информации нужно отнести в первую очередь Конституцию Российской Федерации, в которой в частности сказано: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются»[6],

что подтверждается законом «Об информации, информатизации и защите информации» от 20 февраля 1995 г.

27 июля 2006 года Президентом Российской Федерации были утверждены и подписаны два важнейших для специалистов в области информационной безопасности федеральных закона: № 149 - ФЗ «Об информации, информационных технологиях и о защите информации» и № 152-ФЗ «О персональных данных».

28 июня 2014 года Президентом РФ был утвержден законопроект «Об электронной подписи», который расширил и уточнял положения закона № 149.

Стоит отметить, что наиболее важными документами для сферы туризма и информационной безопасности являются законы РФ:

Федеральный закон «Об основах туристской деятельности в Российской Федерации» является основным актом, регулирующим туристскую отрасль и определяющий права туриста.

В Законе РФ «О защите прав потребителей» говорится, что потребитель имеет право на то, чтобы услуга при обычных условиях ее оказания была безопасна для жизни, здоровья, окружающей среды и имущества потребителя.

Следует отметить, что требование обеспечения сохранности вещей и личных данных постояльцев содержится не только в международных стандартах, а закреплено и в Гражданском Кодексе РФ. На это указывает статья 925 Гражданского Кодекса Российской Федерации:

Для осуществления туристической деятельности необходимо получить лицензию, что предусмотрено ст. 4 Федерального закона «Об основах туристской деятельности в Российской Федерации» и законом «О лицензировании отдельных видов деятельности» от 8 августа 2001 года номер 128-ФЗ.

Основным актом в области стандартизации является Закон РФ от 10 июня 1993 г. «О стандартизации» распространяющийся и на различные виды туристских услуг. Требования, устанавливаемые государственными стандартами для обеспечения безопасности услуг, являются обязательными для соблюдения туристскими организациями. В настоящее время действует ГОСТ р 50644-94 со-

держащий требования по обеспечению личной и информационной безопасности туристов[14].

Именно эти ГОСТы лежат в основе сертификации туристского продукта, являющейся одним из элементов системы регулирования безопасности туризма.

Одной из основных государственных мер обеспечения безопасности в сфере туризма является введение обязательной сертификации туристских и гостиничных услуг. Кодекс РФ об административных правонарушениях предусматривает ответственность должностных лиц и предпринимателей за предоставление несертифицированных услуг. В настоящее время нормативным документом, на основании которого осуществляется сертификация гостиниц, является Приказ Минэкономразвития и торговли РФ от 21 июня 2003г. №197 «Об утверждении положения о государственной системе классификации гостиниц и других средств размещения».

Гражданский кодекс Российской Федерации использует такие понятия, как банковская, коммерческая и служебная тайна. Так, например, в статье 139 говорится, что информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Если обратиться к Уголовному кодексу Российской федерации, то можно обнаружить ряд статей фиксирующих степень ответственности за нарушения в сфере информационной безопасности:

– статья 272. Неправомерный доступ к компьютерной информации;

– статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;

– статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети;

– Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений;

– статья 183 УК РФ аналогична по своему содержанию статье 138 УК РФ, однако, ее действие распространяется на банковскую и коммерческую сферы.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.[9]

Странами, в которых государственная безопасность туризма осуществляется на высоком уровне, являются Мексика, США, Германия и Франция. В России, к сожалению, государственно-отраслевой уровень безопасности в туризме и турбизнесе находится на недостаточной высоте.

1.4 Порядок создания системы обеспечения информационной безопасности в коммерческой организации

Обеспечение безопасности данных включает в себя целый комплекс технических и организационных мер, характеризующихся применением средств защиты информации и решающих задачи предотвращения утечки информации, ее утраты и несанкционированного изменения.

Порядок выполнения работ и организационные функции по обеспечению защиты информации определяются руководителем организации, начальников отделов, которые создают и эксплуатируют объекты информатизации. Контроль эффективности и обнаружение недостатков системы безопасности должно возлагаться на специально назначенное лицо - начальника по защите информации.

Порядок работ по проектированию и эксплуатации совокупности информационных ресурсов, систем обработки информации, а также их средств защиты должен быть зафиксирован в специальном документе «Руководство по обеспечению информационной безопасности», который должен содержать и описывать следующие положения:

– описание и обоснование защищаемой информации;

– описание и обоснование порядка создания, ввода в эксплуатацию и использования ресурсов и средств информатизации;

– утверждение ответственности сотрудников организации за качество их знаний и навыков, а также соответствия их профпригодности требованиям и нормам, установленным в организации.

В организации необходимо наличие официального документа, в котором зафиксирован весь перечень конфиденциальной информации циркулирующей в организации, а также создан порядок доступа к этой информации, согласно правам и обязанностям сотрудников.

Перечислим все этапы разработки системы защиты информации:

– предпроектный этап, состоит из предпроектного исследования объекта, а также должен включать в себя оценочное обоснование важности и необходимости проектирования и внедрения системы защиты информации и технического задания на ее создание. Определяется необходимость обработки конфиденциальных данных на этом объекте, а также перечень сведений ограниченного доступа. Выделяется список технических и программных средств, которые будут использоваться на объекте, а также места их размещения. Проводится аналитическая работа по распределению обязанностей и прав сотрудников по уровню доступа к обработке конфиденциальных сведений;

– этап проектирования – должен включать в себя процесс непосредственного создания и реализации СЗИ в составе объекта информатизации и учитывать финансовые, трудовые и временные ограничения на строительно-монтажные и организационные работы по созданию СЗИ. Данный этап также должен включать в себя необходимость закупки сертифицированного и лицензированного технического и программного обеспечения, а также создание охранной и физической системы защиты помещений и сотрудников организации;

– этап ввода в эксплуатацию СЗИ – должен содержать отладочные и экспериментальные мероприятия СЗИ, а также проверку объекта на соответствие требованиям нормативной документации. Финальным мероприятием по вводу в эксплуатацию СЗИ является аттестация объекта информатизации на соответствие требованиям защиты информации.[8].

Для своевременного обнаружения скрытых угроз безопасности информации, а также с целью максимального усложнения доступа к конфиденциальной информации для злоумышленника необходимо проведение периодического (ежегодного или ежеквартального) контроля над состоянием обеспечения информационной безопасности. Данное мероприятие позволит поддерживать состояние защищенности конфиденциальной информации на стабильно высоком уровне.

Стоит учесть, что в случаях необходимости профессионального анализа на наличие скрытых закладных устройств и иных работ, по решению руководителя организации, могут привлекаться подрядные организации, имеющие соответствующие разращения на такие виды работ, а также положительно зарекомендовавшие себя в области информационной безопасности.[2].

2. Анализ состояния информационной безопасности в отеле «Nevsky Contour»

2.1 Обзор деятельности отеля «Nevsky Contour»

Отель «Nevsky Contour» юридическое название ООО «АТ-Сервис» - это коммерческая организация, находящееся в частной собственности, состоящий из 18ти номеров и предоставляющий гостиничные услуги по временному проживанию с обязательным обслуживанием.

Охарактеризовать гостиницу, как предприятие гостиничной индустрии можно с помощью следующих признаков: номерной фонд, коэффициент загруженности, категоричность, класс обслуживания, а также набор дополнительных услуг.

Номерной фонд отеля представляет собой 18 меблированных комнат из них 1 номер «люкс», что соответствует высшей категории и 17 номеров первой категории, что подразумевает наличие полного санузла в номере.

Коэффициент загруженности используется для характеристики эффективности работы гостиницы и других предприятий размещения туристов. Большое влияние на коэффициент загруженности отеля оказывает сезон различные мероприятия городского, регионального, федерального и международного масштаба.

Процент загрузки номерного фонда отеля рассчитывается как частное от деления количества занятых номеров на общее количество свободных номеров, доступных для проживания (выражается в процентах или долях единицы)[15].

Пример №1. Влияние мирового спортивного события на загрузку отеля.

По формуле 2.1 высчитается загрузка отеля за май 2015 года.

Май 2015г.	
Номерной фонд N	18
Расчетный период (дни) T	31
Продано (занято) за месяц R	466.5
Формула для расчета загрузки Q	R/(N*T)*100%=Q(%)

Q_1=466.5/(18*31)*100%=84% (2.1)

По формуле 2.2 высчитается загрузка отеля за май 2016 года.

Май 2016г (чемпионат мира по хоккею)	
Номерной фонд N	18
Расчетный период (дни) T	31
Продано (занято) за месяц R	519
Формула для расчета загрузки Q	R/(N*T)*100%=Q(%)

Q_2= 519/(18*31)*100%=93% (2.2)

Соотношение показателей загрузок за выбранные года рассчитывается по формуле 2.3.

Q_2-Q_1=93%-84%=9% или 52.5 ночей (2.3)

Увеличение показателя загрузки на 9% несет ощутимую выгоду отелю. При средней стоимости номера в мае 4000руб финансовая разница составляет 52,5*4000=210000руб.

Пример №2. Загрузка отеля в низкий и высокий сезон.

По формуле 2.4 высчитается загрузка отеля низкий сезон 2016 года.

Март 2016г	
Номерной фонд N	18
Расчетный период (дни) T	31
Продано (занято) за месяц R	440.5
Формула для расчета загрузки Q	R/(N*T)*100%=Q(%)

Q= 440.5/(18*31)*100%=79% (2.4)

По формуле 2.5 высчитается загрузка отеля в высокий сезон 2016 года.

Июль 2016г	
Номерной фонд N	18
Расчетный период (дни) T	31
Продано (занято) за месяц R	548
Формула для расчета загрузки Q	R/(N*T)*100%=Q(%)

Q= 548/(18*31)*100%=98% (2.5)

Вне зависимости от сезона отель имеет высокую загрузку более 70%, что подтверждает высокий спрос в любое время года.

Пример №3. Распределение нагрузки по месяцам 2016г показано на графике 2.1.

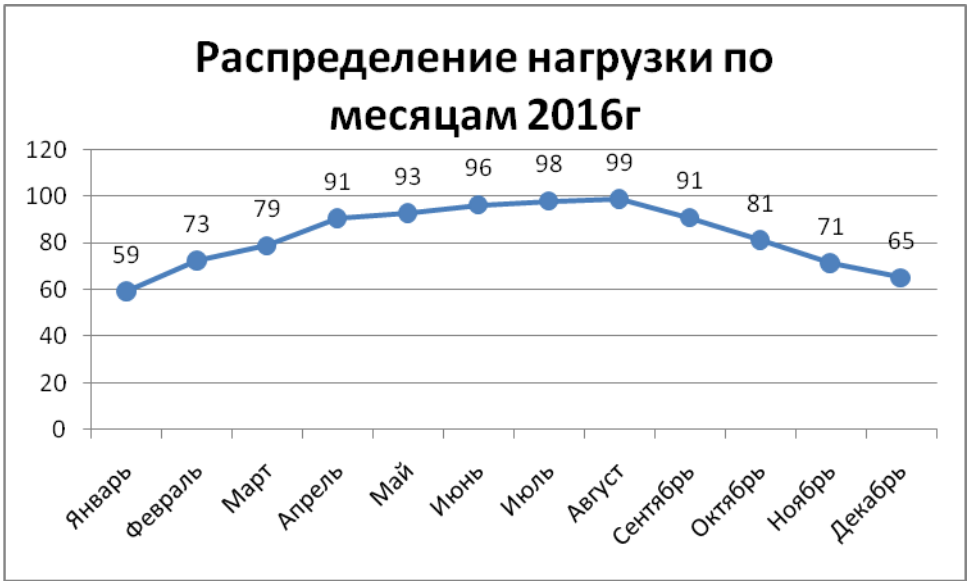


График 2.1- Распределение загрузки по месяцам.

Из графика распределения загрузки видно, что 10 месяцев из 12 загрузка отеля составляет более 70%, что говорит о высокоэффективной организации работы и хорошей репутации отеля.

Классификация гостиниц по категориям основана на комплексе требований к материально-техническому обеспечению, номенклатуре и качеству предоставляемых услуг, уровню обслуживания. В соответствии с приказом Минкультуры России от 11.07.2014 N 1215 "Об утверждении порядка классификации объектов туристской индустрии, включающих гостиницы и иные средства размещения, горнолыжные трассы и пляжи, осуществляемой аккредитованными организациями" (Зарегистрировано в Минюсте России 29.12.2014 N 35473) отелю «Nevsky Contour» присвоена категория три звезды[13].

Класс обслуживания обозначает качество предоставляемых услуг и условно соответствует уровню «туристский класс».

Спектр услуг предоставляемых в отеле:

– Бронирование номеров;
– Прием, регистрация и размещение гостей;
– Прием оплаты за предоставленные услуги и оформление необходи-

мой документации при выезде гостей;

– Оказание разнообразных бытовых услуг гостям;

– Поддержание санитарно-гигиенического состояния номеров;

– Дополнительные услуги: ранний и поздний выезд, звонок-будильник, трансферт, визовая поддержка, завтрак, экскурсионное обслуживание, заказ билетов, охраняемая парковка, хранение багажа, бесплатный Wi-Fi , доставка прессы и т.д..

Согласно нормативной и правовой документации единственным органом управления в ООО «Ат-Сервис» является физическое лицо – руководитель организации, он же генеральный директор.

Перечень его обязанностей составляет:

– Определение направления развития организации;

– Изменение уставных документов;

– Изменение уставного капитала;

– Утверждение ежегодной финансовой документации;

– Решение основных юридических действий (реорганизация и ликвидация организации);

– Представление организации на территории РФ и за ее пределами;

– Распоряжение имуществом и финансовыми активами;

– Утверждение штатных расписаний и финансовыми активами организации.

Непосредственное управление организацией ведет менеджер отеля. В перечень основных его обязанностей входит отчетность о его работе перед руководителем организации, а так же:

– Руководство всеми направлениями деятельности организации;

– Организация работы между структурными подразделениями и производственными единицами;

– Обеспечение неукоснительного выполнения взятых организацией обязательств в рамках договоров с клиентами;

– Осуществление организационного и финансового контроля[16].

Отель «Nevsky Contour» состоит из 3х отделов:

– Отдел службы приема и размещения;

– Финансовый отдел;

– Инженерно-технический.

Организационная структура отеля «Nevsky Contour» представлена на рисунке 2.1.

Отдел обслуживания выполняет функции по бронированию номеров, приему гостей, их регистрации и размещения. Подразделением этого отдела является хозяйственная служба, которая отвечает за поддержание санитарно-гигиеническое состояние номеров, а так же оказание бытовых услуг.

Финансовый отдел занимается вопросами финансового обеспечения предприятия, получает отчеты от кассиров, ведет единый финансовый учет расходов и доходов отеля, проводит операции по учету оплачиваемого рабочего времени и выплачиваемым бонусам. Для выполнения всех функций данного отдела привлечена сторонняя компания.

Инженерно-технический отдел отвечает за техническое оборудование и оснащение гостиницы (системы кондиционирования, теплоснабжения и др.), а так же выполняет функции поддержания порядка и безопасности в гостинице. Для выполнения всех функций данного отдела привлечена сторонняя компания.

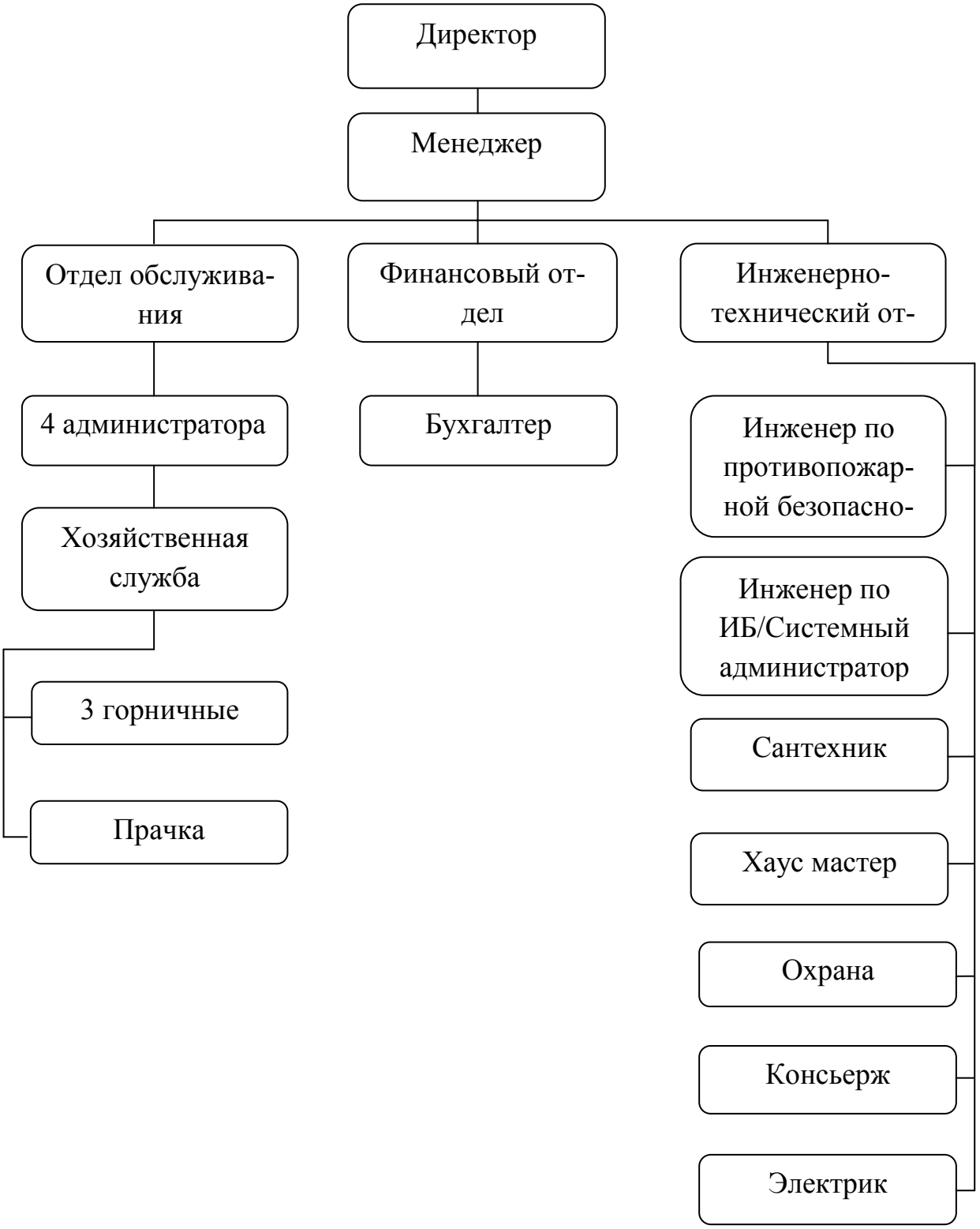
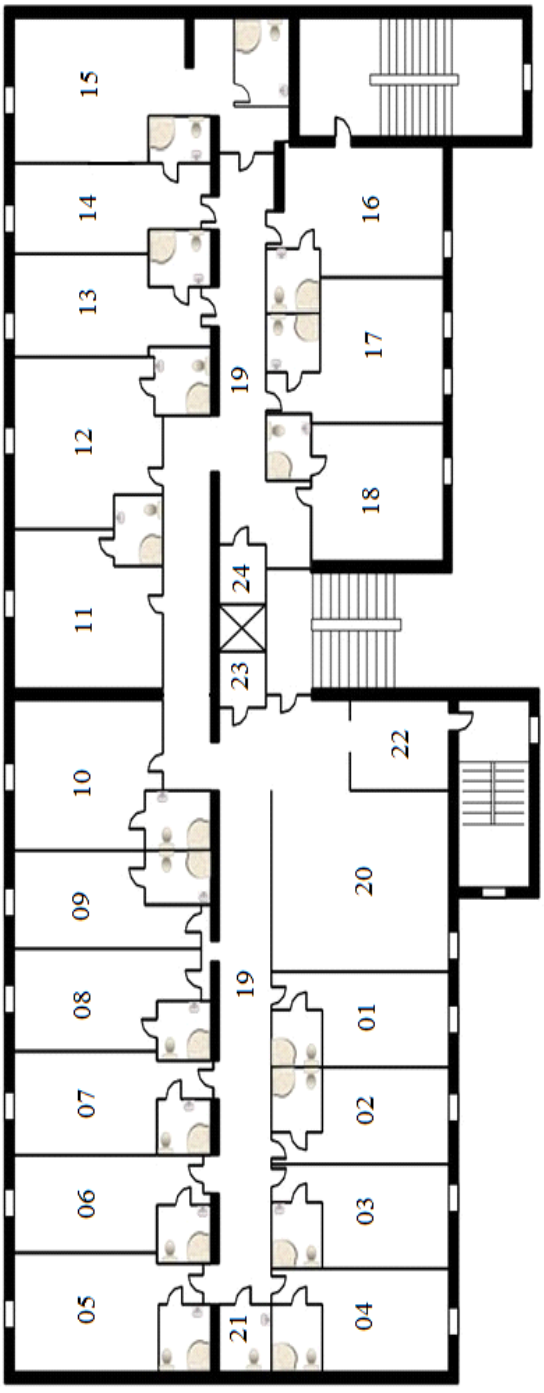


Рисунок 2.1- Организационная структура отеля «Nevsky Contour»

Отель «Nevsky Contour» находится в пятиэтажном здании по адресу: г.Санкт-Петербург, Невский проспект, д.88. Отель занимает третий этаж здания. Организационная структура отеля «Nevsky Contour» представлен на рисунке 2.2.



Условные обозначения	Описание
01-18	Мебелированные номера с собственными санузлами
19	Коридор
20	Отдел обслуживания и рабочее место менеджера
21	Санузел для сотрудников
22	Бумажный архив
23	Серверная
24	Хоз. Часть

Рисунок 2.2- План помещеия отеля «Nevsky Contour»

2.2 Определение информационных потоков в организации

Основным направлением деятельности отеля «Nevsky Contour» является

оказание услуг приема и временного размещения людей.

Для качественного выполнения взятых на себя обязательств отель генерирует, получает, хранит и обрабатывает большой объем данных.

В связи с этим фактом, организации требуется создать надежную систему обеспечения безопасности, которая должна включать:

– Программную и техническую защиту;

– Организационную защиту информации.

В процессе анализа деятельности организации были выявлены информационные потоки, несущие в себе конфиденциальную информацию. Полученные данные приведены в таблице 2.1.

Под информационным потоком следует понимать информацию, в процессе ее движения в пространстве и времени в определенном направлении.

Таблица 2.1-Перечень сведений, составляющих конфиденциальную информацию

№ элемента информации	Перечень данных
1	2
Сведения в области персональных данных	
1	Персональные данные о сотрудниках и постояльцах (ст.3. п.1 №152- ФЗ "О персональных данных")
Сведения в области профессиональной тайны	
2	Информация о клиентах, банковских операциях, номера счетов и кредитных карт.

Продолжение таблицы 2.1

3	Данные из сообщений полученные/отправленные с помощью почтовых сервисов. Информация, доверенная телефонной аппаратуре, включая данные о пользователях, входящих и исходящих звонках и соединениях.
4	Информация о размещении гостей (даты проживания, цены, сопровождающие и т.п.).
Сведения в области бухгалтерского учета	
5	Содержание внутренней бухгалтерской отчетности (ст.10 ФЗ №129 "О бухгалтерском учете")
Сведения, составляющие коммерческую тайну	
6	Сведенья, содержащие клиентскую базу, данные о поставщиках, коммерческие связи.
7	Условия по сделкам и соглашениям, условия контрактов.
8	Сведенья о расчетах тарифов, структуре и расчете цен, о продажной калькуляции, затратах.
9	Сведения о структуре управления, методика обучения персонала.

Продолжение таблицы 2.1

10	Информация об источниках финансирования, а так же сведения о заключенных

	сделках.
11	Сведения, содержащие описание структуры локальной вычислительной сети и полномочий пользователей, обрабатывающих конфиденциальную информацию.
12	Сведения об организации и технических решениях по системе охраны (система контроля доступа) производственных помещений.

Информационные потоки, циркулирующие в отеле «Nevsky Contour», являются смешанными, это означает, что часть информации представлена на бумажных носителях, а часть в виде электронных документов и файлов, которые хранятся в базах данных. Перечень электронных баз данных представлен в таблице 2.2.

Таблица 2.2- Электронные базы данных, использующиеся в отеле «Nevsky Contour».

Наименование электронных баз данных
«БУХта» на основе MS SQL
«ЭЛПОСТ»
Wubook Channel Manager

Формирование баз данных основывается на данных полученных от клиентов и сотрудников отеля.

Клиенты обращаются в отель «Nevsky Contour» за предоставлением услуг приема и размещения. Все клиенты делятся на 2 типа: Физические и Юридические. Служба приема и размещения ведет работу непосредственно с физическими лицами, а менеджер с юридическими.

Для бронирования номеров в отеле «Nevsky Contour» можно использовать электронные формы на всемирных сайтах, таких как booking.com, expedia.com, agoda.com, ostrovok.com и других. Вся информация о клиенте (даты периода проживания, контактная информация, цель визита, место проживания и даже платежные данные) будет занесена в базу данных менеджера каналов Wubook и хранится там до конца существования отеля, за исключением платежной информации, которая подлежит еженедельной чистке.

При заезде клиент и отель заключают между собой договор в одном экземпляре (который остается у отеля) об оказании услуг по временному размещению с одной стороны и своевременной оплаты с другой. Данные об оплатах, списках проживающих, свободных/занятых номерах, оказанных услугах, продажах сопутствующего товара и т.д. отображены в комплексе «БУХта» со сроком хранения данных равным сроку функционирования отеля.

Согласно статье 20 Федерального закона, отель обязан ставить на миграционный и регистрационный учет всех клиентов, пользующихся услугами временного размещения. Для этого существует автоматизированная система «ЭЛПОСТ» предназначенная для электронной передачи данных о регистрации или снятии с регистрационного учета по месту пребывания. Электронный вариант хранится в системе один год с момента выезда из отеля.

С юридическими лицами ведет работу менеджер отеля. Для оказания услуги подготавливается договор в 2х экземплярах, шаблоны договоров хранятся в «БУХте». После уточнения нюансов с директором отеля «Nevsky Contour», договора передаются на подпись второму участнику соглашения, после чего один вариант остается у юридического лица, а второй доставляется обратно в отель почтой либо курьером. Все сведенья об операциях с юридическими лицами заносятся в систему учета «БУХта».

После оказанных услуг, бухгалтером подготавливаются документы на оплату и уже после оплаты составляются акты выполненных услуг, подписание которых говорит о соглашении обеих сторон с выполнением всех услуг в полном объеме.

Информационные потоки в отеле «Nevsky Contour», которые протекают во время оказания услуг, представлены на рисунке 2.3 .

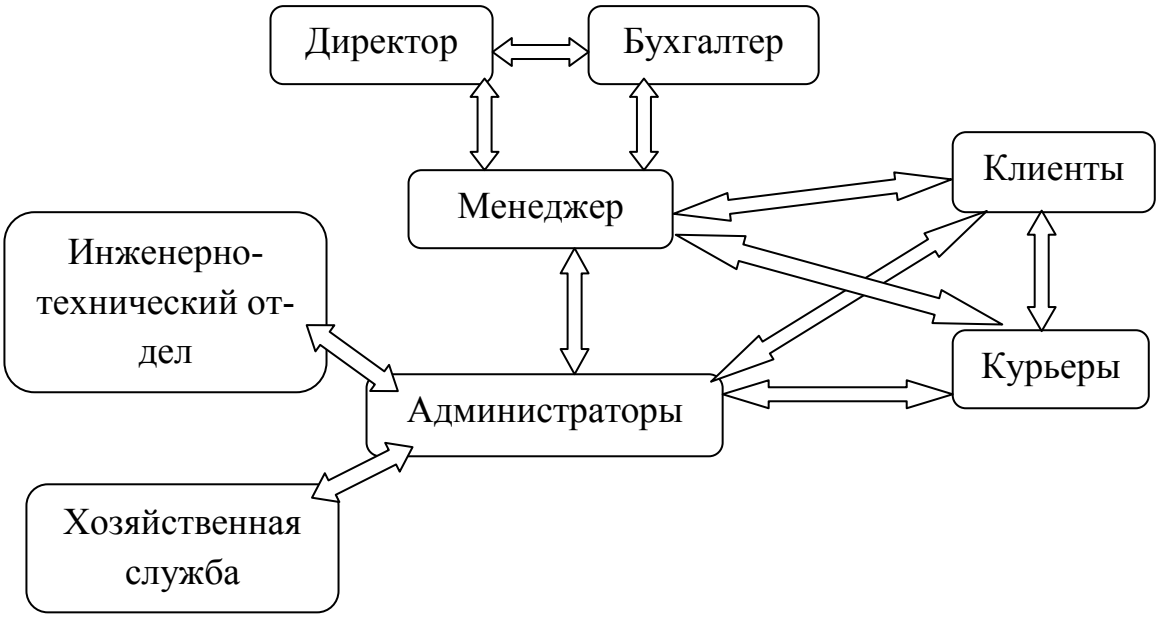


Рисунок 2.3 - Информационные потоки, связанные с оказанием услуг

Так же в отеле «Nevsky Contour» информация циркулирует между менеджером и бухгалтером. Документы, поступающие от менеджера к бухгалтеру, заносятся в базу данных «БУХта». Кроме этого бухгалтер ведет учет сотрудников и создает карточку бумажного дела сотрудника. После удаления данные о сотрудниках стираются из базы, а бумажное дело передается в архив и хранится согласно закону об архивном деле.

Формирование отчетов для директора о выдаче заработной платы сотрудникам, для Пенсионных и Налоговых органов. Информация передается в Пенсионные и Налоговые органы в зашифрованном виде с помощью программного обеспечения КриптоПро CSP по открытым каналам связи.

Потоки информации, связанные с бухгалтерским учетом, представлены на рисунке 2.4.

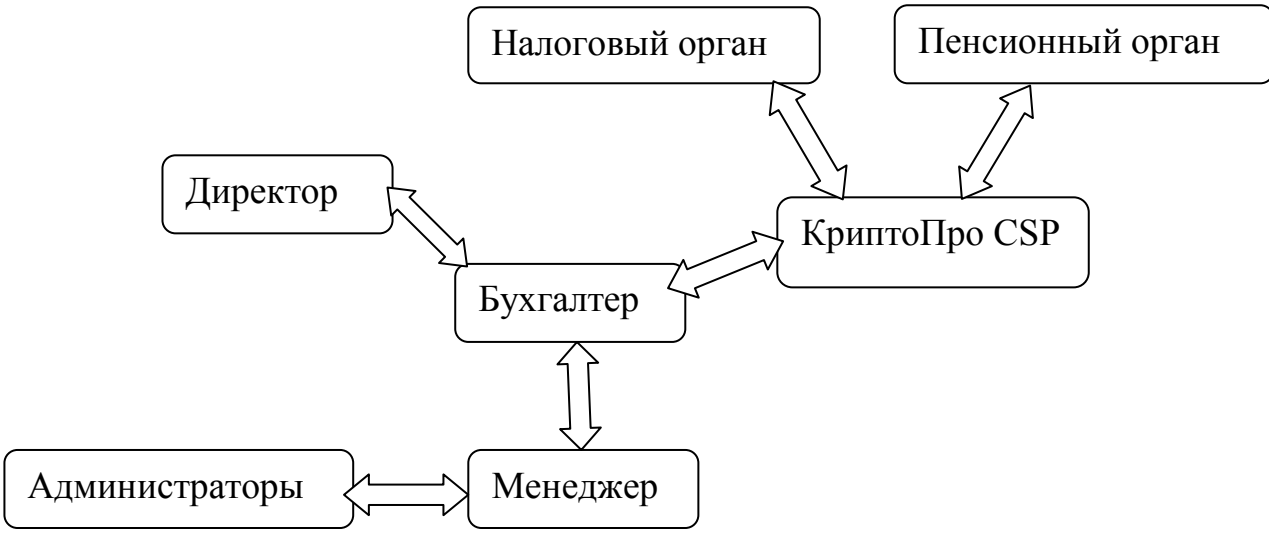


Рисунок 2.4 – Информационные потоки, связанные с бухгалтерским учетом

В отеле «Nevsky Contour» многие из указанных выше информационных потоков содержат конфиденциальную информацию, а так же информацию, которую не рекомендуется разглашать согласно организационным регламентам.

2.3 Анализ состояния защищенности отеля «Nevsky Contour»

В ГОСТ №15971-90 «Системы обработки информации. Термины и определения» даются следующие определения:

– обработка информации - систематическое выполнение операций над данными, представляющими предназначенную для обработки информацию;

– системой обработки информации - совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, обеспечивающая выполнение автоматизированной обработки информации;

– технические средства системы обработки информации - все оборудование, включая носителя данных, предназначенное для автоматизированной обработки информации;

– передача информации - физический процесс, посредством которого осуществляется перемещение информации в пространстве;

– хранение информации - процесс передачи информации во времени, связанный с обеспечением неизменности состояний материального носителя информации (бумаги, фотоплёнки, магнитного диска, и т. п.).[4]

В отеле «Nevsky Contour» под средствами обработки, хранения и передачи информации понимается совокупность электронно-вычислительного оборудования.

В отеле имеется 3 компьютера («АРМ-1…3»), одна телефонная станция и один сервер. В распоряжении персонала приема и размещения находится один персональный компьютер, второй компьютер находится у менеджера и третий у бухгалтера. Все ЭВМ объединены в одну локально вычислительную сеть.

2.4 Обоснование естественных угроз безопасности информации

Естественными угрозами информационной безопасности являются стихийные бедствия и явления, не поддающиеся влиянию человека, например: пожары, удары молний, наводнения, ураганы и другие.

Среди естественных угроз наиболее часто встречаемыми и наиболее опасными с точки зрения потери данных являются пожары. Для предотвращения потерь информации посредством угроз пожара, обязательным условием является оборудование помещений противопожарными датчиками и средствами пожаротушения. Помимо этого на любом предприятии должен быть назначен специалист ответственный за противопожарную безопасность.

Если помещение, в которых находятся носители ценной информации (серверы, архивы, носители цифровых данных и пр.), располагается в критической близости к водоемам, то существует угроза потери информации вследствие наводнения.

Влияющим фактором на вероятность потери информации от какого-либо вида естественных угроз является особенность географического положения. К примеру, вероятность землетрясения или цунами в Японии колеблется в облас-

ти 50%, а в центральной части России менее 1%. [4]

2.5 Обоснование искусственных угроз безопасности информации

К искусственным угрозам информационной безопасности относятся угрозы, вызванные действиями человека. Выделяют два типа искусственных угроз: преднамеренные и не преднамеренные.

Угрозы называются непреднамеренными или случайными, если действия совершены по неосторожности, невнимательности, незнанию или обыкновенного любопытства. Установка программ на компьютер не входящих в список необходимых для работы относится к непреднамеренным угрозам, так как это действие может стать причиной нестабильной работы системы и потери информации.

Преднамеренными угрозами или умышленными называются угрозы, вызванные действиями со злым умыслом. Сюда можно отнести внешние и внутренние атаки от агентов организаций-конкурентов, либо собственных сотрудников, например не довольных статусом в фирме или заработной платой.

Согласно аналитическим исследованиям центра InfoWatch за первое полугодие 2016 года было зарегистрировано 840 случаев утечки конфиденциальной информации, из которых 49,1% - случайные утечки и 50,9%- умышленные. В сравнении с аналогичным периодом 2015 года зафиксирован незначительный рост доли умышленных утечек по отношению к случайным. Это говорит о необходимости применения защитных мер не только от умышленных действий нарушителей, но и от случайных угроз[17]. Доли случайных и умышленных утечек показаны в диаграмме 2.1 и 2.2 на основе таблицы 2.3.

Таблица 2.3- Соотношение случайных и умышленных утечек.

Типы утечек	Год	
	2015	2016
Умышленные	45.2	50.9
Случайные	54.8	49.1

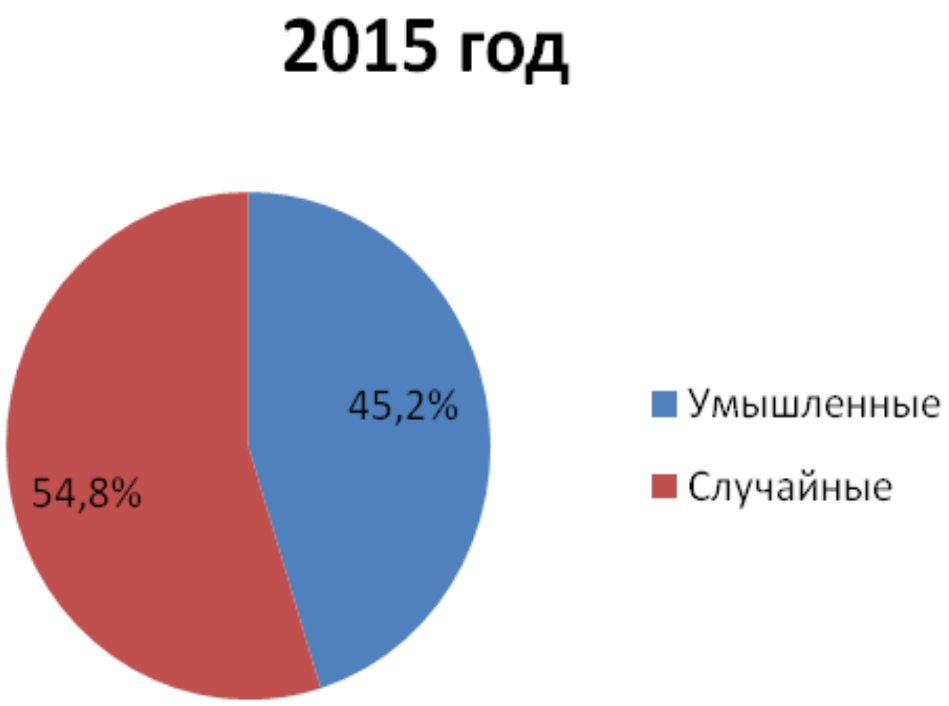


Диаграмма 2.1- Соотношение случайных и умышленных утечек за 2015 год

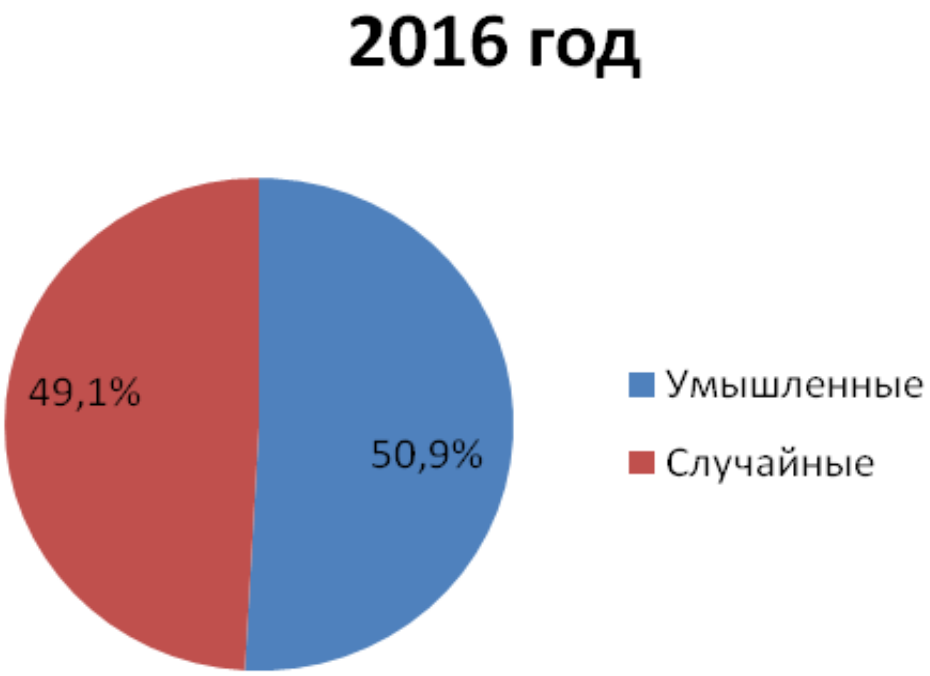


Диаграмма 2.1- Соотношение случайных и умышленных утечек за 2015 год

Внешние и внутренние атаки имеют основную общую цель- получение несанкционированного доступа к конфиденциальной информации организации. Данные цели осуществимы при помощи использования программных и технических каналов утечки информации.

Технические каналы утечки информации можно классифицировать по их физическим характеристикам:

- радиоэлектронные КУИ;
- акустические КУИ;
- оптические КУИ;
- материально-вещественные КУИ.

2.6 Оценка эффективности существующей системы безопасности информации в отеле «Nevsky Contour».

Одним из самых распространенных каналов утечки информации на любом предприятии является оптический канал утечки, в котором можно получить информацию путем фотосъемки, видеосъемки или даже путем

элементарного подглядывания, слежки. Это связано с тем фактом, что современные оптические приборы имеют большое разрешение, которое может передавать изображения с высоким уровнем детализации даже на очень удаленном расстоянии от объекта разведки. Стоит отметить, что оптические каналы могут быть зафиксированы в диапазонах видимого, инфракрасного и ультрафиолетового спектров.

К оптическим каналам утечки информации в отеле «Nevsky Contour» относятся компьютерные мониторы, информация на бумажных носителях, графические изображения и схемы, а так же изображения отраженные в зеркалах и глянцевых поверхностях. К оптическому каналу утечки информации злоумышленники могут получить доступ, используя специальное разведывательное оборудование через окна и открытые двери помещений отеля. Существует возможность установки скрытых камер видеонаблюдения, но она не велика, так как общие помещения отеля оборудованы камерами слежения и при выявлении попытки установки, разведывательные устройства будут незамедлительно ликвидированы. Вход в отель оборудован пропускной системой, но это не может полностью исключить возможность проникновения злоумышленников на территорию отеля.

Весьма информативным может стать акустический канал утечки информации с точки зрения несанкционированного съема конфиденциальных данных.

Наличие уязвимостей в акустическом канале обусловлено неконтролируемым распространением звуковых волн в звукопроводящих средах.

В отеле «Nevsky Contour» возможно наличие конфиденциальных разговоров в отделе обслуживания, на рабочем месте менеджера и в бумажном архиве.

Анализ материально-вещественного канала утечки информации показал, что, прежде всего, внимания заслуживает неправильная политика утилизации документов на бумажных и электронных носителях и аппаратуры. Утилизация или продажа офисной техники может таить опасность утери конфиденциаль-

ных данных. Это связано с невозможностью полного уничтожения данных при попытках удаления только стандартными службами операционной системы.

В отеле «Nevsky Contour» материально-вещественный канал утечки информации локализован не полностью. Утилизация бумажных, магнитных и иных носителей осуществляется не должным образом, не смотря на то, что на них возможно содержание информации с ограниченным доступом.

Радиоэлектронными источниками утечки данных в отеле «Nevsky Contour» являются такие информационные каналы, которые возникают за счет широкого вида побочных электромагнитных излучений и наводок (ПЭМИН), которые образуются вследствие эксплуатации компьютерного оборудования. ПЭМИН – определяется физическими процессами, которые возникают в окружающей среде в результате работы электроприборов и радиоприборов.

На первый взгляд данный канал утечки информации можно оценить как менее опасный, на пример по сравнению с акустическим, но не стоит забывать, что почти все коммерческие тайны организации проходят этапы обработки на персональных компьютерах. Съем уязвимых данных от работающего компьютерного оборудования возможен при использовании средств радио и радиотехнической разведки, которые расположены за пределами контролируемой зоны организации.

Каждая работающая ЭВМ в отеле «Nevsky Contour» создает разночастотные побочные излучения. При помощи специальных средств злоумышленник может получить доступ к данным излучениям и оценив их характеристики способен выявить полезную информативную составляющую.

В отеле «Nevsky Contour» каждая ЭВМ обрабатывает и хранит стратегически важную и конфиденциальную информацию. Поэтому все компьютеры в отеле следует обезопасить от возможности несанкционированного доступа по каналу ПЭМИН.

Все помещение, которое занимает отель, оборудовано противопожарной системой.

Наряду с традиционными техническими каналами утечки информации повышенную уязвимость информационной системы создают так называемые «виртуальные» каналы утечки информации, при внедрении злоумышленника в программную среду ЭВМ.

Стандартное программное обеспечение любой универсальной компьютерной системы включает три основные компоненты: операционная система, сетевое аппаратное обеспечение и система управления базами данных[18]. Исходя из этого, в таблице 2.4, выделены три группы попыток взлома компьютерных систем.

Таблица 2.4 - Группы попыток взлома компьютерных систем

	Тип атаки	Методы НДС
1	Атаки на уровне сетевого программного обеспечения	- Прослушивание сегмента локальной сети; - Перехват сообщений на маршрутизаторе или создание ложного марщрутизатора; - Отправка в сеть сообщений с ложным обратными сетевыми адресами, злоумышленник переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей; - Отправка в сеть сообщений специального вида. При этом компьютерные системы, подключенные к сети, полностью или частично выходят из строя.

Продолжение таблицы 2.4

2	Атаки на уровне систем управления базами данных	-Реализация НДС на уровне операционной системы, что позволяет получить доступ к файлам СУБД с помощью средств операционной системы; -Преодоление защиты на уровне СУБД (когда СУБД не имеет достаточно надежных защитных механизмов).
3	Атаки на уровне операционной системы	- Получение пароля: из файла, в котором пароль был сохранен пользователем; кража внешнего носителя парольной информации и т.д.; подглядывание при вводе пароля; - Сканирование жестких дисков компьютера; - Восстановление ранее удаленных объектов (если позволяют средства операционной системы); - Превышение полномочий; - Отказ в обслуживании (частичный или полный вывод из строя операционной системы).

2.7 Экономическое обоснование системы защиты информации

Получение прибыли – это та цель, которую ставят перед собой любые коммерческие организации. Поэтому систему защиты информации нужно спроектировать и внедрить таким образом, что бы это получилось экономически выгодно и обоснованно. Можно описать целесообразность системы защиты информации через несколько экономических показателей организации:

- объем реализации услуг;

- экономия от снижения издержек;
- текущие издержки организации;
- прибыль.

Экономическая целесообразность внедрения СЗИ в организацию должна быть рассчитана с учетом потенциального ущерба вследствие кражи или утечки конфиденциальной информации[19].

На этапе проектирования правильный расчет стоимости системы обеспечения информации позволяет вносить правки с целью расширения финансирования, или, наоборот, с целью экономии.

Исходя из отсутствия общепринятой системы распределения грифов секретности к разным типам конфиденциальной информации на коммерческих предприятиях, генеральным директором отеля «Nevsky Contour» было принято решение о классификации всей конфиденциальной информации по трем кластерам и присвоения каждому классу грифы конфиденциальности: начальный, основной, усиленный. Каждому грифу конфиденциальности была определена в соответствие условная цена на единицу информации (Мбайт):

- начальный – 500 руб.;
- основной – 1500 руб.;
- усиленный – 2500 руб.;
- наивысший – 3000 руб.

Цена конфиденциальных данных определяется в соответствии с представленной формулой 2.1:

$C=V*Z$

Где C – цена защищаемой информации в условных единицах;

V – объем защищаемой информации в мегабайтах;

Z – цена за 1 мегабайт информации;

Данные по стоимости и объему информационных объектов представлены в таблице 2.5.

Таблица 2.5 – Объем и стоимость элементов информации

Перечень данных	Объем, Мбайт.	Гриф	Цена за единицу инф. в соответствии с грифом, руб.	Цена инф., руб.
Сведения о структуре управления, методика обучения персонала.	10	Начальный	500,00	5 000,00
Информация об источниках финансирования, а так же сведения о заключенных сделках.	10	Начальный	500,00	5 000,00
Персональные данные о сотрудниках и постояльцах	500	Основной	1 500,00	750 000,00
Информация о клиентах, банковских операциях, номера счетов и кредитных карт.	500	Наивысший	3 000,00	1 500 000,00

Продолжение таблицы 2.5

Сведения, содержащие описание структуры локальной вычислительной сети и полномочий пользователей, обрабатывающих конфиденциальную информацию.	10	Наивысший	3 000,00	30 000,00
Сведения об организации и технических решениях по системе охраны (система контроля доступа) производственных помещений.	20	Наивысший	3 000,00	60 000,00
Информация о клиентах, банковских операциях, номера счетов и кредитных карт.	500	Наивысший	3 000,00	1 500 000,00
Сведенья, содержащие клиентскую базу, данные о поставщиках, коммерческие связи.	500	Начальный	500,00	250 000,00

Продолжение таблицы 2.5

Данные из сообщений с помощью почтовых сервисов. Информация, доверенная телефонной аппаратуре, включая данные о пользователях, входящих и исходящих звонках и соединениях.	1000	Начальный	500,00	500 000,00
Информация о размещении гостей (даты проживания, цены, сопровождающие и т.п.).	500	Основной	1 500,00	750 000,00
Содержание внутренней бухгалтерской отчетности.	200	Усиленный	2 500,00	500 000,00
Условия по сделкам и соглашениям, условия контрактов.	400	Начальный	500,00	200 000,00
Сведенья о расчетах тарифов, структуре и расчете цен, о продажной калькуляции, затратах.	10	Основной	1 500,00	15 000,00
Итого:				4 565 000,00

Общий объем конфиденциальных данных приведен в таблице 2.6.

Таблица 2.6- Общий объем конфиденциальных данных

Гриф конфиденциальности	Объем, Мб.
Начальный	1920
Основной	1010
Усиленный	200
Наивысший	520

Соотношение объема конфиденциальной информации по выделенным грифам показано на диаграмме 2.3.

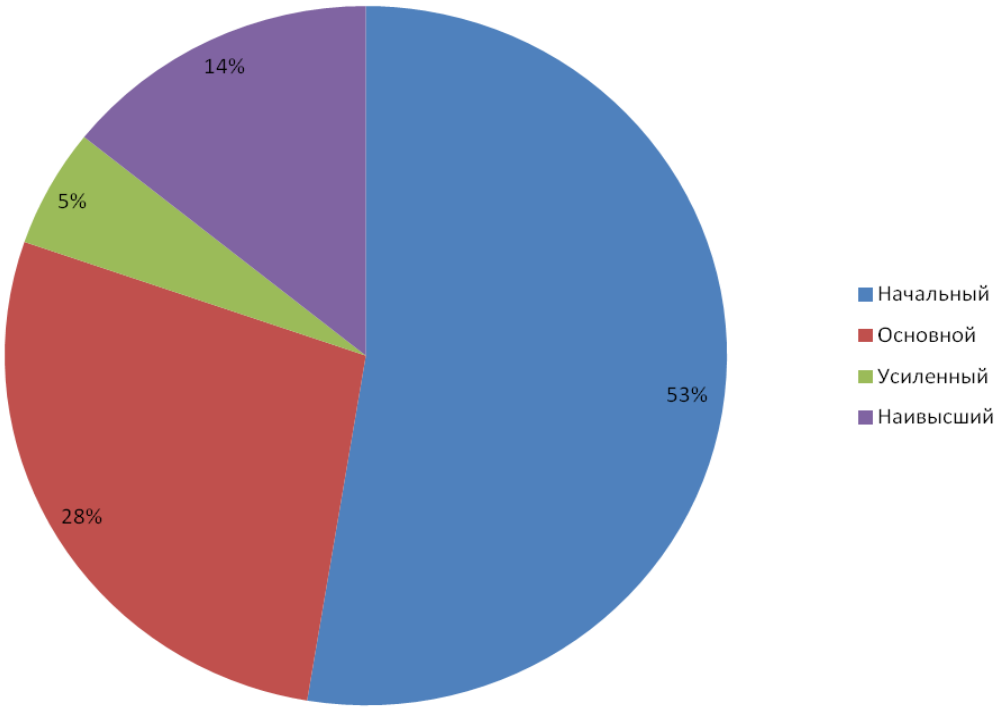


Диаграмма 2.3 - соотношение объемов данных информации.

Таким образом, отель «Nevsky Contour» постоянно располагает данными на общую сумму 4 565 000 рублей. В этой сумме не учтена оценочная стоимость важной информаций и других ценности, которыми может располагать каждый постоялец отеля.

Ранее проведенный анализ состояния информационной безопасности выявил, что существует возможность несанкционированного доступа к конфиденциальной информации. Путем экспертной оценки была выявлена общая стоимость циркулирующей информации в отеле «Nevsky Contour», которая составляет внушительную сумму в 4 565 000 рублей. Исходя из этого было установлено, что создание системы обеспечения безопасности – полностью экономически обоснованное мероприятие.

3 Проектирование системы обеспечения информационной безопасности в отеле «Nevsky Contour».

3.1 Обоснование методов и средств обеспечения информационной безопасности

Сегодня в руках профессионалов гостиничного дела сосредоточено большое количество разнообразных средств по борьбе с преступлениями. На современном рынке средств информационной безопасности достаточно широко представлено оборудование и программное обеспечение от простых и бюджетных моделей, до уникальных и дорогих комплектов и систем. Исходя из этого, любой организации без затруднений можно подобрать наиболее подходящие ей средства защиты информации учитывая свои потребности.

Анализ каналов утечки информации позволил локализовать все угрозы информационной безопасности:

- оптический съем данных через окно;
- оптический и акустический съем данных через открытую дверь;
- перехват ПЭМИН;
- получение доступа к документам, при неправильной утилизации;
- хакерские атаки и использование компьютерных вирусов;
- кража ценных вещей и документов.

Для достижения полной защиты информации отеля следует локализовать все выявленные угрозы.

Наиболее эффективный и экономичный способ решения проблемы оптической утечки информации через оконные проемы в помещениях с циркулирующими конфиденциальными данными - это установка жалюзи, что позволяет исключить возможность утечки информации через окна.

Выделить оптимальный вариант жалюзи для отеля позволяет анализ коммерческих предложений поставщиков и производителей жалюзи.

В таблице 3.1 перечислены популярные образцы жалюзи и их цены.

Таблица 3.1 –Список образцов жалюзи и их цены

Производитель	Материал	Цена за 1 м2 (руб.)
LDStyle	Ткань	690
	Пластик	990
	Алюминий	2590
VD дизайн	Ткань	640
	Пластик	1170
	Алюминий	2790
SVIL	Ткань	630
	Пластик	1218
	Алюминий	2665
Жалюзи Град	Ткань	590
	Пластик	1185
	Алюминий	2580
СПБ жалюзи	Ткань	635
	Пластик	1480
	Алюминий	2280

В административной части отеля имеется только одно окно размером 3метра на 1,5 метра, поэтому, опираясь на качественные характеристики и стоимость продукции, выбор падает на тканевые жалюзи компании «Жалюзи Град». Жалюзи будут устанавливаться на площадь окна 4,5м2, следовательно стоимость жалюзи составит 2 655руб.

Установка доводчиков на каждую дверь помещений как жилых, так и административных, позволит исключить возможность утечки информации сразу по 2м каналам: акустическому и оптическому. Благодаря этой мере снизится вероятность слежки методом подслушивания и подсматривания. Наиболее оптимальные образцы доводчиков дверей представлены в таблице 3.2.

Кроме этого необходимо расположить столы и рабочее оборудование таким образом, что бы у злоумышленника не было невозможности видеть мониторы компьютеров. Дополнительным решением для защиты мониторов от посторонних глаз является защитная пленка, которая уменьшает угол обзора до 60 градусов. Данное средство защиты можно приобрести в Российском подразделении интернет магазина мировой компании «3М» по цене 1950 руб./штука. В отеле имеется 3 ЭВМ, стоимость оснащения данными девайсами каждой электронно-вычислительной машины составит 5850руб.

Таблица 3.2 – Список образцов дверных доводчиков и их цена.

Образец доводчика двери	Характеристика	Цена (руб.)
MSM D 180	Доводчик рекомендован к установке на двери весом от 170 до 190 килограмм. Морозостойкий с ветровым тормозом, есть регулировка скорости довода и закрывания.	1875

Продолжение таблицы 3.2

FALCON EYE FE-B4W	Доводчик рекомендован к установке на двери весом от 65 до 85 килограмм. Диапазон рабочих температур от -42 до +55 градусов. Не требует перенастройки при больших перепадах	1750

	температур и влажности. Есть регулировка скорости открытия, закрытия и «дохлопа».	
«Зубр»	Подходит к установке, как на левые, так и на правые двери массой до 80 килограмм. Возможна раздельная регулировка скоростей доводки и закрытия двери. Возможно использование в отрицательных температурах благодаря морозостойкой гидравлической жидкости внутри доводчика.	1429
EXIT E-602	Доводчик рекомендован к установке на двери массой до 70 килограмм. Диапазон рабочих температур от +40 до -35 градусов, устойчив к погодным воздействиям благодаря специальному порошковому покрытию. Имеется регулировка скоростей в двух диапазонах.	887

Продолжение таблицы 3.2

DORMA TS-71	Доводчик подходит к установке, как на правые, так и на левые двери массой до 80 килограмм. Рекомендован к использованию от -15 градусов Цельсия. Имеется две независимые регулировки скорости закрывания в двух диапазонах.	2645

Основываясь на вес и габариты дверей, было выбрано два образца доводчиков, MSM D 180 с установкой на входные двери и FALCON EYE FE-B4W для установки на межкомнатные двери.

На территории отеля имеется 25 дверей, на которые необходимо установить доводчики, из которых 3 входные двери и 22 межкомнатные. Общая цена доводчиков для 25 дверей составит 44 125 рублей.

Для возможности утилизации бумажных носителей без возможности последующего извлечения из них информации требуется приобрести уничтожители бумаги-шредеры. Для отеля «Nevsky Contour» достаточно установить один шредер в отделе обслуживания. В таблице 3.3 представлены наиболее подходящие модели уничтожителей бумаги.

Таблица 3.3 – Список образцов уничтожителей бумаги и их цена

Образец шредера	Характеристики	Цена (руб.)
Fellowes Powershred P-48C	Персональный шредер емкостью корзины 18 литров с механическим датчиком пуска. За один раз может измельчать по 8 листов со скоростью нарезки 3,6 м/мин. Размер частицы на выходе 3,9мм на 50 мм. Мощность шредера 57Вт.	7380
Office Kit S 145	Офисный шредер повышенной конфиденциальности позволяет уничтожать конфиденциальную информацию с высокой степенью секретности. Перекрестный тип нарезки позволяет измельчать бумагу до размеров 2мм на 15мм. Емкость корзины 20 литров. За один раз может измельчать 10-11 листов бумаги со скоростью нарезки 3,3м/мин. Мощность шредера 185Вт. Есть отделение для уничтожения CD и пластиковых карт. Автоматическое выключение при перегреве.	16000

Продолжение таблицы 3.3

Fellowes MicroShred 450M	Персональный шредер высокого уровня секретности с рекомендуемым количеством переработки в день: бумаги-50 листов, кредитных карт-25штук, CD и DVD-10штук. Измельчает бумагу до размеров 2мм на 15мм со скоростью 2.1 м/мин. Емкость корзины 22 литра.	20720
REXEL AUTO+60X	Офисный шредер с возможностью одновременной загрузки до 60 листов и емкостью корзины 15 литров. Измельчает бумагу до размеров 4мм на 45мм со скоростью 1,5м/мин, так же есть возможность измельчения кредитных карт, CD и DVD.	11050
BURO BU-C968N	Шредер с повышенной степенью секретности и возможностью загрузки до 8 листов одновременно. Емкость корзины 30 литров. Измельчает на фрагменты 2мм на 8 мм. Есть возможность измельчения кредитных карт, CD и DVD.	15760

Ориентируясь на специфику деятельности отеля, было принято решение о приобретении аппарата Office Kit S 145 стоимостью 16000руб.

Что бы исключить возможность кражи или не правильного использования важной документации или других ценностей отеля, было принято решение ус-

тановить два сейфа в бумажном архиве. Один из них для пользования администраторами, второй только менеджера и генерального директора. Постояльцы отеля тоже нуждаются в надежном хранении собственных ценностей, в связи с этим было принято решение о закупке 18ти сейфов для установки в каждый номер. В таблице 3.4 представлены наиболее подходящие сейфовые хранилища.

Таблица 3.4 – Список образцов сейфов и их цена.

Наименование сейфа	Характеристики	Цена (руб.)
VALBERG AW 2714	Встраиваемый сейф с ключом. Габариты 270x330x145 мм. Объем 5 литров. Вес 10 кг. Замок защищен от высверливания. Сейф имеет порошковое покрытие и усиленные внутренние петли. Устойчивость к взлому - ГОСТ Р 50862-2005.	6100
РИПОСТ-С24	Встраиваемый сейф с ключом. Габариты 230x360x190 мм. Вес 10кг. Сейф с порошковым покрытием и одной внутренней полкой. Устойчивость к взлому - ГОСТ Р 50862-2005.	6300

Продолжение таблицы 3.4

AIKO SH-28 EL	Сейф с анкерным креплением к полу или стене. Габариты 280х340х317 мм. Объемом 24 литра и весом 13 кг. Сейф имеет порошковое покрытие. Оснащен электронным замком со звуковыми и визуальными сигналами. Работа сейфа поддерживается 4мя батарейками. Программируется шифром и имеет аварийный мастер-ключ. Устойчивость к взлому - ГОСТ Р 50862-2005.	6900
SFT-20 EA	Сейф мебельный с порошковым покрытием и возможностью крепления к полу. Габариты 190х300х150 мм. Объем 8 литров. Работа на электроном замке с защитой от взлома со звуковыми и визуальными сигналами. Работа сейфа поддерживается 4мя батарейками, при этом встроена энергонезависимая память событий. В комплекте предоставляется ключевой замок KABA MAUER. Устойчивость к взлому - ГОСТ Р 50862-2005.	3500

Продолжение таблицы 3.4

VALBERG ASM 46	Сейф с анкерным креплением к полу или стене. Габариты 460х440х355 мм. Объемом 60 литров и весом 27кг. Сейф имеет порошковое покрытие с ключевым типом замка. В комплекте предоставляется ключевой замок KABA MAUER. Устойчивость к взлому по ГОСТ Р 55148-2012.	10100
AIKO TM 63 EL	Подстольный сейф с возможностью анкерного крепления к полу или стене. Габариты 630х440х355 мм. Объемом 66 литров и весом 34 кг. Сейф имеет порошковое покрытие с защитой замка от высверливания. Работа основана на электронном кодовом замке в комплекте с аварийным мастер-ключом. Устойчивость к взлому - ГОСТ Р 50862-2005.	10500

Из всех рассмотренных образцов сейфов, было решено закупить и установить 18 сейфов модели SFT-20 EA , 1 сейф модели VALBERG AW 2714 для пользования администраторов и 1 сейф модели VALBERG ASM 46 для пользования менеджера и генерального директора. Общая стоимость 20 сейфов составит 79200 рублей.

Неконтролируемое распространение конфиденциальных данных по каналу ПЭМИН блокируется с помощью использования специальных устройств защиты - генераторов шума. В Российской Федерации уделяется большое внимание вопросам подавления побочных электромагнитных излучений и наводок,

поэтому современный рынок достаточно широк в плане выбора подобных устройств.

В таблице 3.5 представлены наиболее подходящие средства по борьбе с ПЭМИН.

Таблица 3.5 – Список образцов генератора шума.

Генератор шума	Характеристика	Цена (руб.)
Соната-Р2	Генератор шума работает в диапазоне частот от 0,01МГц до 2000МГц с потребляемой мощностью 10 Вт. Коэффициент качества шума не менее 0.8.	16000
ЛГШ-505	Генератор шума работает в диапазоне частот от 0,01 МГц до 1000 МГц с потребляемой мощностью не более 55Вт. Поддерживается круглосуточная работа прибора. Средний срок службы 10 лет. Коэффициент качества шума не менее 0.6.	14600

Продолжение таблицы 3.5

ГШ-К-1800	Генератор шума работает в диапазоне частот от 0,01 МГц до 1800 МГц. Срок службы около 10 лет. Коэффициент качества шума не менее 0.8.	8300
SEL SP-113 Блокада	Генератор шума работает в диапазоне частот от 0,01 МГц до 2000 МГц. Коэффициент качества шума не менее 0.8.	16300
ШТОРА-1	Генератор шума работает в диапазоне частот от 0,01 МГц до 1500 МГц с потребляемой мощностью не более 25Вт. Возможно электропитание от автомобильного прикуривателя мощностью 12 В. Коэффициент качества шума не менее 0.8.	57000

В результате анализа всех средств защиты от побочных электромагнитных излучений и наводок, было принято решение о приобретении генератора шума «ГШ-К-1800». Данное средство сможет обеспечить защиту от утечки информации по каналу ПЭМИН в радиусе приблизительно 50метров.

Стоимость выбранного генератора шума «ГШ-К-1800» составляет 8300рублей.

Компьютеры пользователей и сервер отеля являются хранилищем для всей важной информации, во избежание непреднамеренной потери данных, было принято решение об организации резервного копирования на внешний отказоустойчивый носитель. В таблице 3.6 представлены наиболее подходящие системы резервирования информации.

Таблица 3.6 – Список систем резервного копирования

Система резервного копирования данных	Характеристики	Цена (руб.)
Pervasive backup agent	Программное обеспечение обеспечивает мощную защиту данных от потерь, повреждений или удаления. Это ПО обладает высокой надежностью, защищенностью и производительностью клиент-серверной архитектуры, предлагает все возможности серверной СУБД на одном ПК без ущерба производительности. Программа встраиваема в приложения, которые работают на движках SQL. Все операции шифруются 128-битным ключом.	14816

Продолжение таблицы 3.6

Paragon Drive Backup 14 Server	Программное обеспечение, использующее последние разработки в области создания резервных копий ОС и данных. Осуществляет резервное копирование Windows без прерывания работы, владеет высоким уровнем совместимости с ОС, ПО и всеми видами накопителей информации. Эффективный инструментарий осуществляет легкую миграцию данных на виртуальные и физические носители, все циркулирующие данные шифруются и защищаются паролями. Бессрочная лицензия.	13164
Acronis Backup 12 Server License incl. AAP ESD	Самое простое и быстрое резервное копирование в мире для защиты всех данных. Можно восстанавливать отдельные сообщения электронной почты, папки, документы, базы данных и целые системы. Все данные проходят операцию шифрования, при этом восстановление данных происходит мгновенно. Бессрочная лицензия с технической поддержкой.	26219

Продолжение таблицы 3.6

Handy Backup Server Network	Одно из лучших решений для среднего бизнеса, имеющее возможность централизованного бэкапа и восстановления удаленного сервера. Быстрый откат систем в работоспособное состояние. Бессрочная лицензия с технической поддержкой.	63750
Ontrack EasyRecovery	Данное По позволяет легко и без труда восстановить данные с флэшкарт, оптических дисков, смартфонов, жестких дисков и другое. В комплекте поставляется аварийная дискета для восстановления данных, когда нет возможности восстановить систему Windows обычными способами. Бессрочная лицензия и техническая поддержка.	24990

Из всех рассмотренных средств восстановления данных было выбрано программное обеспечение «Pervasive backup agent» от разработчика Pervasive Software.

Для обеспечения информационной безопасности локальной сети не достаточно применения, какого либо одного программного или аппаратного средства, эта проблема требует комплексного подхода.

При организации работы отеля, отказ оборудования не должен считаться чрезвычайной ситуацией. Возникновение данной ситуации предусмотрено заранее и были приняты меры внедрения RAID массива пятого уровня, который сможет минимизировать финансовые потери или конфликтные ситуации с клиентами, связанные к примеру, с простоем системы. Стоимость внедрения дан-

ного оборудования 18000рублей. Структурная схема RAID массива пятого уровня показана на рисунке 3.1.

Для надежности хранения данных, с помощью утилиты TrueCrypt 7.0, было выполнено шифрование данных. Наиболее удачным алгоритмом шифрования (с точки зрения влияния на производительность процессора и надежность) был выбран алгоритм AES с длинной ключа 256бит.

Всю большую популярность, не только среди предприятий, но и среди обычных пользователей, набирают виртуальные частные сети (VPN), их используют для решения проблем безопасного обмена данными при передаче их по открытой сети.

Для фильтрации входящих пакетов данных и принятия решения об их попадании в локальную сеть из глобальной применяется межсетевой экран. Данная фильтрация осуществляется с помощью набора правил, определяющих условия прохождения пакетов с данными через так называемую границу между сетями. Использование межсетевых экранов позволяет организовать внутреннюю политику сети предприятия.

Стандартные программные решения не требуют дополнительных материальных затрат для внедрения виртуальной частной сети или межсетевого экрана в уже существующую локальную сеть. Схема подключения VPN с межсетевым экраном показана на рисунке 3.3.

Для локализации проблем с вирусными и хакерскими атаками, на рабочие станции и сервер должны быть установлены антивирусные программы. В таблице 3.7 представлены наиболее подходящие антивирусные системы для закупки и внедрения на организации.

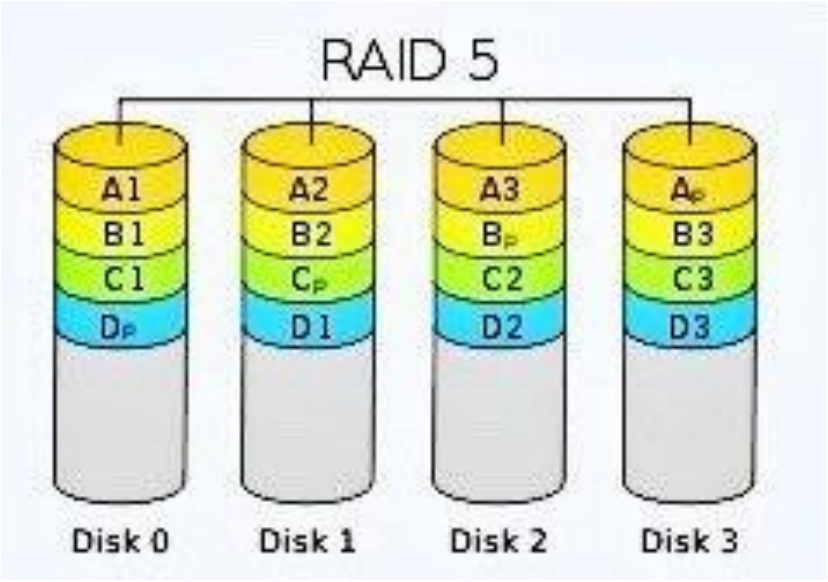


Рисунок 3.1 – Структурная схема RAID-массива

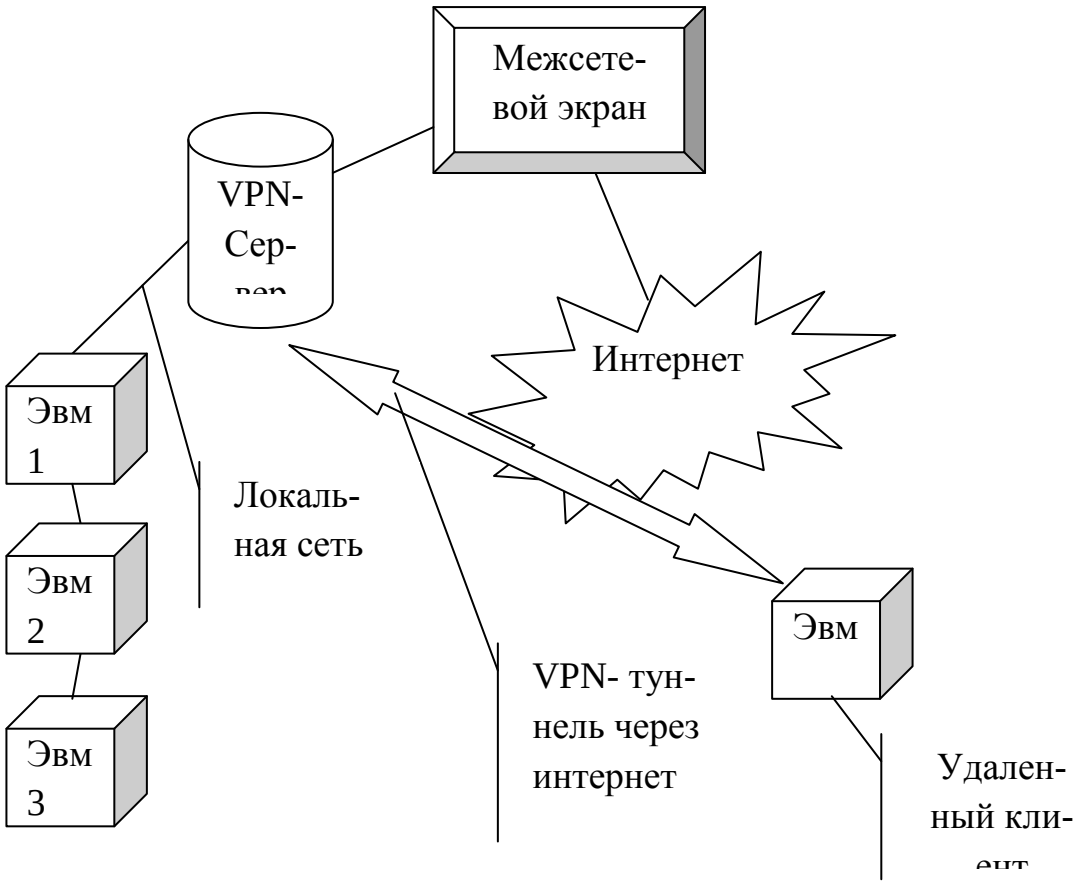


Рисунок 3.3 – Схема реализации виртуальной частной сети с межсетевым экраном в отеле «Nevsky Contour».

Таблица 3.7 – Список антивирусных систем и их цена.

Наименование СЗИ	Основные характеристики	Цена (руб.)
Dr. Web Enterprise Security Suite 10.0	Централизованная защита всех узлов сети: рабочие станции, почтовые, файловые сервера и сервера приложений, включая терминальные, интернет-шлюзы и мобильные устройства. Благодаря встроенному антивирусу, антиспаму, брандмауэру и офисному контролю, осуществляется комплексная защита рабочих станций от большинства существующих угроз.	40 568
Kaspersky Endpoint Security	Бизнес-решение для обеспечения IT-безопасности рабочих станций и файловых серверов со встроенными инструментами контроля рабочих мест. Контроль и защита мобильных устройств реализуется за счет централизованного управления системой защиты.	39 600

Продолжение таблицы 3.7

ESET NOD32 Secure Enterprise	Программное обеспечение с централизованной защитой от интернет-угроз, тоянских программ, шпионского и рекламного программного обеспечения, фишинга и тд.. Бизнес-решение для централизованной защиты рабочих станций, мобильных устройств и файловых серверов Обеспечивает высокий уровень безопасности корпоративной сети (рабочие станции, мобильные устройства и файловые сервера) без снижения ее быстродействия.	69 783
Symantec Anti-Virus Corporate Edition for Workstations and Servers	Бизнес-решение для обеспечения безопасности всего предприятия с внедрением предовых технологий защиты от вирусов и программ-шпионов. Устранение побочных эффектов позволяет компьютерам работать в обычном режиме, даже если в системе их защиты появилась брешь.	20692

В конечном итоге, основываясь на следующие факторы: международный рейтинг, возможности платформы, стоимость с ПО, было принято решение о приобретении антивирусной системы Kaspersky Endpoint Security.

Для обеспечения контроля доступа на объект необходимо приобрести два комплекта СКУД и установить его на входную дверь на лестничной площадке. В комплект системы контроля доступа входит следующее оборудование:

– автономный контроллер

– считывающее устройство
– электронный замок
– доводчик двери
– ключи
– кнопка выхода
– блок питания

Выбор автономных котроллеров достаточно широк, однако среди подобных устройств существует несомненный лидер – это контроллер Z-5R. Он представляет собой компактное устройство с достаточно богатым функционалом. Схема подключения всех узлов к контроллеру Z-5R представлена на рисунке 3.4.

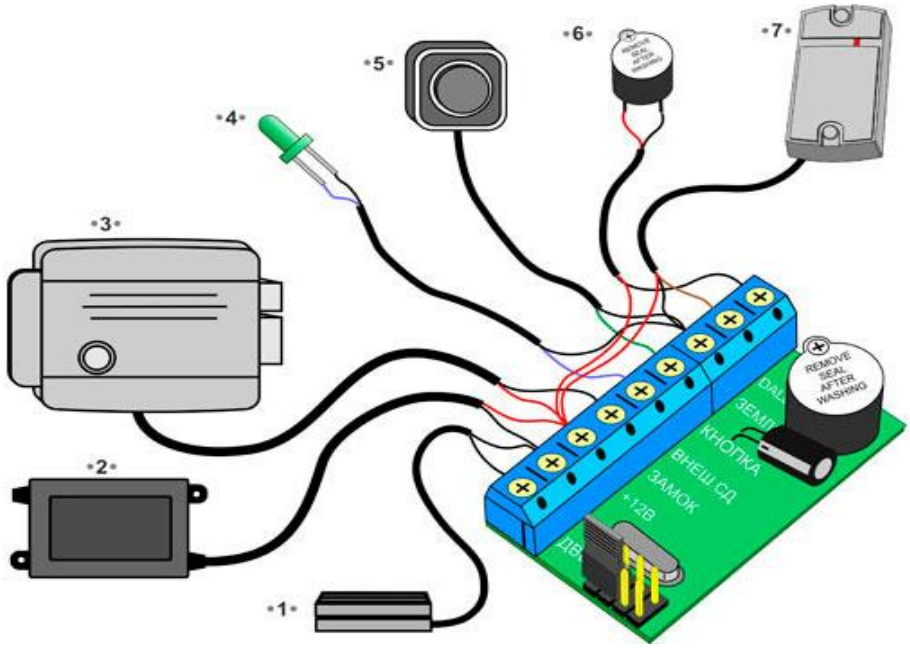


Рисунок 3.4 – Система контроля и управления доступом

Стоимость отдельных компонентов СКУД представлена в таблице 3.8.

Таблица 3.8 – Стоимость компонентов СКУД

Наименование	Описание	Цена (руб.)
1	2	3

Контроллер Z-5R	Автономный контроллер для ограничения доступа в административные и промышленные помещения. Возможно подключение контактного считывателя ключей, бесконтактного считывателя proximity-карт, электромагнитного/механического замка/защелки, кнопки открывания, внешнего зуммера и светодиода и датчика открытой двери. Может работать с большим количеством ключей. Так же есть возможность вести базу ключей на ПК. Существует установка длительности открытия замка.	400
Электромагнитный замок ML300-50	Представляет собой корпус с электромагнитом и ответную металлическую пластину. Обычно пластина крепится на двери, а замок на дверной коробке. При снятии напряжения питания замка дверь отпирается.	1960

Продолжение таблицы 3.7

Дверной доводчик MSM D 180	Доводчик рекомендован к установке на двери весом от 170 до 190 килограмм. Морозостойкий с ветровым тормозом, есть регулировка скорости довода и закрывания.	1875
Ключ доступа (20 шт.)	Бесконтактный ключ доступа. Пластиковый брелок с тиснением логотипа.	520
Кнопка выхода	Накладная, вандалозащищенная кнопка в металлическом корпусе, цвета меди.	260
Источник электропитания БП-1А	Источник питания БП-1А рекомендован к использованию при температурах от +5 до +40 градусов Цельсия. Предназначение-питание электромеханических замков различного типа и устройств управления замком.	370

Таким образом, стоимость одного комплекта СКУД составит 5385 рублей. Монтаж и программирование системы контроля и управления доступом будет выполняться инженерно-техническим отделом.

3.2 Определение мест размещения средств обеспечения информационной безопасности

Во второй главе был представлен план помещения отеля «Nevsky Contour» и согласно особенностям планировки отеля разработаем схему расположения всех ЭВМ и средств защиты.

Для обеспечения защиты конфиденциальных данных циркулирующих в отеле следует применить следующие средства:

- тканевые жалюзи компании "Жалюзи град";
- доводчики для входных дверей модели "MSM D 180";
- доводчики для межкомнатных дверей модели "FALCON EYE FE-B4W";
- защитная пленка на экраны компьютеров компании "3M";
- уничтожитель бумаги "Office Kit S 145";
- сейфы для клиентов модели SFT-20 EA, сейф для администраторов модели VALBERG AW2714, сейф для менеджера и генерального директора VALBERG ASM 46;
- генератор шума "ГШ-К-1800";
- система резервного копирования "Pervasive backup agent" от разработчика Pervasive Software;
- внешний отказоустойчивый носитель;
- установка межсетевого экрана, виртуальной частной сети и антивирусной системы;
- комплект оборудования СКУД.

В свободный слот шины PCI материнской платы компьютера устанавливается плата генератора шума "ГШ-К-1800".

Полный список принятых мер по борьбе с возможными угрозами представлены в приложении Б.

Для предотвращения утечки информации по оптическому каналу необходимо изменить месторасположение компьютеров в отделе приема и размеще-

ния, что бы изображения на экранах были не доступны для посторонних глаз.

Схема расположения ЭВМ и средств защиты представлена в приложении Б.

Так же для предотвращения утечки информации по оптическим каналам необходимо расположить ЭВМ в отделе обслуживания таким образом, чтобы мониторы компьютеров были недоступны для глаз посетителей.

План расположения всех ЭВМ и средств защиты представлен в приложении Б.

3.3 Разработка организационной и управленческой структуры информационной безопасности

Важным этапом для любой организации, которая заботится о сохранности конфиденциальных данных, является разработка организационно-управленческой структуры безопасности. Правильность планирования и реализация этого этапа позволит обеспечить согласованность действий каждого сотрудника в рамках коллектива, увеличить скорость всех бизнес-процессов связанных с информационной безопасностью и поддерживать безопасность на требуемом уровне. Исходя из этого, эффективность созданной системы безопасности напрямую зависит от грамотной управленческой, контролирующей и организационной работы.

В предыдущих разделах данной дипломной работы был проведен анализ системы обеспечения безопасности отеля «Nevsky Contour», на основе выявленных недостатков были выбраны и утверждены руководителем отеля программные и аппаратные средства устраняющие недочеты системы безопасности. Главными факторами при выборе оборудования и программных средств послужили: стоимость, набор функций и экономичность. Не смотря на все предпринятые меры, информационная безопасность будет считаться не состоятельной без проведения грамотной управленческой и организационной работы.

Начало управленческой работы было положено с назначения генерального директора отеля ответственным за создание, поддержку и реализацию сис-

темы информационной безопасности. В его обязанности входит:

– создание, внедрение и поддержка политики безопасности отеля;

– пересмотр политики безопасности в связи с изменением внешних или внутренних условий. Такими условиями могут считаться появление новых угроз безопасности, требования законодательства или государственных органов, изменение технической структуры организации;

– контроль выполнения требований системы обеспечения безопасности.

Несколько раз в год генеральным директором отеля «Nevsky Contour» должен быть инициирован перепросмотр функционирующей системы информационной безопасности и исходя из этого подготовка отчетной документации, а именно:

– отчет динамики развития системы информационной безопасности, то есть сравнение эффективности усовершенствованной системы с эффективностью систем прошлых проверок;

– отчет по инцидентам, которые были зафиксированы в системе информационной безопасности;

– отчет с оценками технологических новинок в области защиты информации.

Централизованное и координированное внедрение системы обеспечения информационной безопасности и ее эксплуатация возможно только при наличии управляющих лиц:

– менеджер отеля «Nevsky Contour»;

– инженер по обеспечению информационной безопасности;

Основными задачами выполняемые советом по безопасности информации являются:

– определение функций и задач для каждого должностного лица организации;

– согласование по применению методов и технологий защиты информации (прогнозирование возможностей несанкционированного доступа, обнаружение и слежение за новыми информационными потоками, распределение информации по грифам секретности);

– анализ новых средств в области информационной безопасности;

– обоснование необходимости применения инновационных средств защиты от утечек;

– проведение мероприятий для повышения квалификации и уровня знаний в области обеспечения информационной безопасности;

– контроль нарушения информационной безопасности во всех существующих и создаваемых проектах организации;

– проведение анализа инцидентов нарушения информационной безопасности;

– публичная демонстрация поддержки обеспечения информационной безопасности в компании[4].

Согласно внутреннему распорядку за выполнением распоряжений генерального директора и совета по информационной безопасности за состоянием информационной безопасности на местах несут ответственность и следят сотрудники приема и размещения.

Советом по информационной безопасности отеля «Nevsky Contour» были установлены:

– информационные ресурсы, которые используются информационными автоматизированными системами;

– списки сотрудников, использующие те или иные информационные системы;

– уровни доступа определенных сотрудников к информационным системам.

Информационными ресурсами, которые используются автоматизированными информационными системами, являются:

– файловые и реляционные базы данных;

– инструкции и справочная документация к информационным системам; прикладное программное обеспечение;

– системное программное обеспечение, а также инструментальные средства разработки и утилиты; [3].

Вся информация подлежит классификации для дальнейшего определения ее приоритетности, необходимости и степени защиты, данное действие необходимо для обеспечения информационной безопасности на надлежащем уровне. С особым вниманием следует отнестись к конфиденциальной информации, которая требует дополнительного уровня защиты или специального метода обработки. Классификация информации дает возможность определения способа обработки и защиты, а система классификации информации позволяет определить соответствующее множество уровней защиты и потребность в специальных методах обработки.

Приказом генерального директора отеля «Nevsky Contour» создается комиссия для проведения классификации автоматизированных систем. Результатом работы комиссии является Акт классификации автоматизированной системы.

Система доступа представляет собой совокупность норм и правил, определяющих, кто из руководителей организации, кому из пользователей и с какими категориями документов может давать разрешение на ознакомление [4].

Система доступа должна отвечать следующим требованиям:

– обоснованность доступа к конфиденциальным документам, т.е. доступ, является обоснованным, когда он базируется на служебной необходимости;

– возможность предоставления всех необходимых документов и информационных ресурсов для выполнения конкретного вида работы (в силу служебных обязанностей);

– обеспечение только санкционированного доступа к документам, т.е. осуществление доступа, осуществляется только после разрешения на то

уполномоченного лица. При этом уполномоченное лицо может давать разрешение на доступ сотрудникам, исключительно входящими в сферу его деятельности и только установленному кругу лиц [3].

Во время заключения трудового договора между отелем и предполагаемым сотрудником, работодатель должен осведомить о том, что выполнение трудовых обязанностей тесно связано с манипуляциями над коммерческой тайной. Исходя из этого, при приме на работу, каждый сотрудник должен подписывать соглашение о неразглашении коммерческой тайны как неотъемлемую часть трудового договора.

При подписании данного соглашения сотрудник, должен быть ознакомлен с ответственностью, которую он понесет в случае непредумышленного и умышленного распространения конфиденциальной информации. Сила ответственности истекает не менее чем через три года после освобождения сотрудника от занимаемой должности.

Отдельным пунктом соглашения должны быть вынесены применяемые меры воздействия на сотрудника в случае возникновения инцидента нарушения информационной безопасности.

На регулярной основе каждый сотрудник отеля должен проходить соответствующие обучения и стажировки связанные с обновлениями политик и процедур информационной безопасности, утвержденных организацией.

Обучение сотрудников обеспечивает:

– знание требований информационной безопасности;

– знание ответственности в соответствии с законодательством;

– правильную эксплуатацию средств обработки информации (процедуры регистрации в системах, использование пакетов программ и т.д.) [3].

Инженер обеспечения информационной безопасности обязан следить за тем, чтобы каждый сотрудник имел четкое представление о различных видах инцидентов нарушения информационной безопасности, умели правильно реагировать на них и своевременно сообщать о них инженеру по обеспечению безопасности.

Инженер обеспечения информационной безопасности назначается ответственным за периодическое методическое обучение и инструктаж персонала.

По результатам проведенного инструктажа с персоналом, каждый из них должен быть подготовлен к демонстрации полученных знаний и навыков перед инженером обеспечения информационной безопасности.

3.4 Оценка эффективности разработанной системы технической защиты средств обработки, хранения и передачи информации

Третья глава данного дипломного проекта была посвящена разработке системы информационной безопасности в отеле «Nevsky Contour» для оценки ее эффективности следует провести повторный анализ состояния информационной защищенности отеля по результатам проведенных работ.

Во время анализа разных типов угроз информационной безопасности в отеле «Nevsky Contour» были выявлены следующие каналы утечки информации:

- радиоэлектронные КУИ;
- акустические КУИ;
- оптические КУИ;
- материально-вещественные КУИ.

Для локализации выявленного канала утечки информации ПЭМИН было закуплено и введено в эксплуатацию специальное оборудование генератор шума "ГШ-К-1800".

Для защиты информации от утечки по выявленным акустическим каналам были применены доводчики дверей двух типов : MSM D 180 для входных дверей, Falcon EYE FE-B4W для межкомнатных дверей.

Утечка важной информации по оптическим каналам не возможна, так как были применены различные средства и методы защиты. Возможность съема информации через окна устранена при помощи установки жалюзи от компании "Жалюзи Град". Защита мониторов от посторонних глаз осуществлена с помощью специальных защитных пленок компании "3М". Исходя из этого оптиче-

ский канал утечки информации, можно считать полностью устраненным.

Локализация материально-вещественного канала утечки информации осуществлена посредством ввода в эксплуатацию уничтожителя бумаги Office Kit S 145, который способен утилизировать диски и бумажные документы механическим образом. Для хранения важных документов и носителей информации используются сейфы. Так же с сотрудниками была проведена методическая работа, в рамках которой им была объяснена опасность неконтролируемой утилизации документов и носителей информации.

Для защиты информации на компьютерах, сервере и в локальной сети отеля «Nevsky Contour» было установлено соответствующее программное обеспечение и технические средства: система резервного копирования "Pervasive backup agent", VPN, межсетевой экран, антивирус Kaspersky Endpoint Security,отказоустойчивые RAID-массивы с шифрованием AES.

Для обеспечения контроля доступа было приобретено и установлено два комплекта системы контроля и управления доступом с установкой на входную дверь и на дверь в бумажный архив.

Исходя из анализа каналов утечки информации, можно сделать вывод, что все существующие угрозы локализованы. И на данный момент возможность утечки конфиденциальной информации отсутствует.

Основываясь на проведенные финансовые расчеты, было выявлено, что в вычислительных средствах отеля «Nevsky Contour» циркулирует информация на общую сумму 4 565 000 рублей.

Закупка, установка и настройка средств защиты информации для отеля «Nevsky Contour» обойдется в 357 453 рублей.

Чистая годовая прибыль отеля «Nevsky Contour» в несколько десятков раз больше суммы необходимой для создания системы защиты информации. Генеральный директор отеля «Nevsky Contour» считает эти траты разумными и полностью обоснованными.

Исходя из вышесказанного, можно сделать вывод о том, что спроектированная система защиты информации, циркулирующая в средствах обработки,

хранения и передачи информации в отеле «Nevsky Contour» эффективна и сумма, необходимая для реализации проекта, не значительна.

4 Технология управления процессами обеспечения безопасности в отеле «Nevsky Contour»

4.1 Структурно-функциональная схема объекта обеспечения безопасности

Рассматриваемым объектом обеспечения безопасности выступает отдел приема и размещения отеля «Nevsky Contour».

Рассматриваемый объект - рабочее место администраторов и менеджера.

На рабочем месте администратора и менеджера необходимо провести оценку эргономических условий.

На рисунке 4.1 с условными обозначениями схематично показано расположение компьютеров.

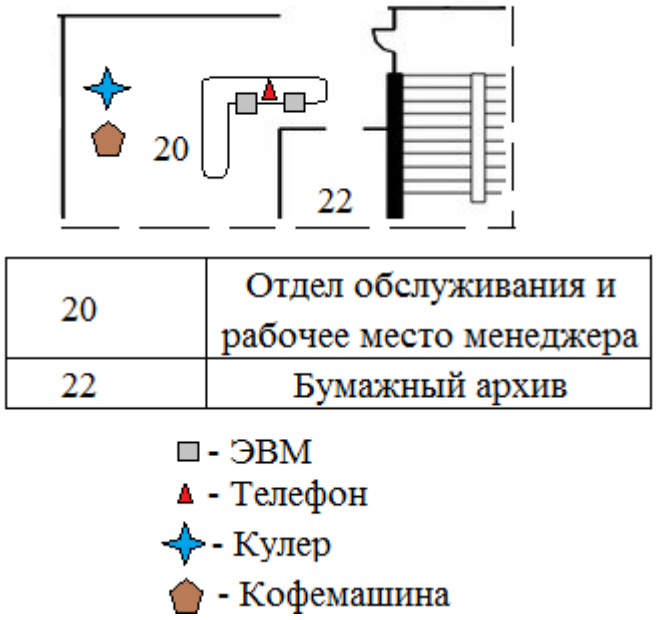


Рисунок 4.1- Схема расположения компьютеров.

Нарушения эргономических условий:

При проведении оценки эргономических условий на рабочем месте администраторов и менеджера был выявлен ряд нарушений и несоответствий эргономическим нормам.

В отделе обслуживания клиентов ярко выраженное нарушение микроклиматического режима, что ухудшает состояние и работоспособность. Влаж-

ность воздуха в помещении – 19-26%, что ниже минимально допустимого значения в 40%.

В пользовании администраторов находится принтер. Принтер располагается в рабочей зоне работника. Он находится на расстоянии вытянутой руки. Яркость поверхности принтера составляет 625 кд/м2, что в 3 раза превышает норму – 200 кд/м2.

Стойка ресепшен не соответствует требованиям для работы с ПЭВМ. Глубина стола составляет 600 мм, при минимально установленном значении глубины – 800 мм. Из-за этого сокращается расстояние между монитором, установленным на столе и глазами пользователя. Так же за мониторами установлены светодиодные лампы, яркость которых отрицательно сказывается на работоспособности администраторов. Из-за недостаточной глубины рабочей поверхности и большого объема обрабатываемой информации, на столах скапливается много документации. Данное обстоятельство не позволяет полностью класть руку на стол, что может стать причиной переутомления или травмы.

Рабочее кресло имеет маленькую амплитуду регулировки, из-за чего работникам с ростом выше 170см приходится наклонять голову вниз для работы за компьютером. Из-за чего возможно развитие сколиоза и болезней шейного отдела позвоночника. Не смотря на это, кресло дает возможность быстро и легко перемещаться в рабочей зоне.

На рабочем месте отсутствует обязательная подставка для ног. Из-за её отсутствия у работников наблюдается неправильное положение ног относительно корпуса, нагрузка на ступни распределяется неравномерно.

Данные показатели существенно влияют на принятие удобной, комфортной рабочей позы.

4.2 Методика проведения оценки эргономических условий на рабочих местах сотрудников приема и размещения.

Порядок выполнения работы:

1. Заполнение индивидуальной карты рабочего места сотрудников приема и размещения.

2. Визуальный осмотр помещения и рабочего места.

3. Проведение измерений и внесение результатов в таблицы.

Измеряемые параметры:

- размер помещения;
- освещение;
- микроклимат;
- рабочая зона;
- рабочий стол;
- рабочий стул;
- подставка для ног;
- монитор;
- клавиатура и мышь;
- системный блок;
- тяжесть трудового процесса;
- напряжённость трудового процесса.

4. Проведение отчётов и внесение результатов в таблицы.

5. Анализ полученных результатов[23].

4.3 Основные характеристики

Визуальный осмотр помещения показал, что место работы сотрудников оборудовано:

– Регулируемыми жалюзи;
– Системой отопления;
– Аптечкой;
– Системой приточно-вытяжной вентиляции;
– Системой кондиционирования воздуха;
– Пожарной сигнализацией;
– Кнопкой вызова охраны;

– Системой видеонаблюдения.

Характеристики визуального осмотра рабочего места работников показал:

– Свет от оконного проема падает сзади;

– Отсутствует подставка для ног.

Характеристики помещения:

– S(LSD ВДТ/ЭТЛ ВДТ)=4,5-6,0м^2;

– V($I_а$-$I_б$/$II_а$-$II_б$) =15/25м^3.

Характеристики освещения:

– Яркость потолка, стен, светильников, поверхностей экрана и поверхностей стола равна 200кд/м^2;

– Яркость бликов стола и экранов компьютеров равна 40кд/м^2;

– Освещенность в зоне расположения рабочего документа равна 300-500 лк;

– Освещенность поверхности экрана равна до 300 лк;

– Показатель ослеплённости общего освещения равен 40;

– Коэффициент пульсации общего освещения равен 5%.

Характеристики микроклиматических условий:

– Температура воздуха в теплый период равна 20-25°С;

– Температура воздуха в холодный период равна 22-24°С;

– Относительная влажность 40-60%;

– Скорость движения воздуха 0,1 м/с.

Характеристики рабочей зоны:

– Высота стойки ресепшена (разделительной перегородки) 1,5м.

Характеристики рабочего стола:

– Отсутствие острых краев;

– Матовая (полуматовая) фактура поверхности стола;

– Глубина стола не менее 800см;

– Длина одного рабочего места 1200см[20].

Характеристики рабочего стула:

– Закругленный передний край;

– Полумягкая поверхность сиденья, спинки и подлокотников;

– Нескользящее не электризующееся, воздухонепроницаемое покрытие;

– Возможность съема подлокотников;

– Регулируемая высота;

– Изменение угла наклона спинки на 30%[20].

Характеристики подставки для ног:

– Рифленая поверхность;

– Регулировка высоты и угла[20].

Характеристики монитора:

– Дисплей ниже глаз пользователя и на расстоянии 600-700 см;

– Возможность поворота по вертикали и горизонтали;

– Матовый корпус однородного цвета;

– Антибликовое покрытие;

– Регулировка яркости и контраста[21].

Характеристики клавиатуры:

– Матовый корпус однородного цвета;

– Наличие ножек и возможность изменения угла положения от 0° до 15°[21].

Характеристики системного блока:

– Матовый корпус однородного цвета;

– Удаленность от приборов отопления;

– Расстояние между торцом стола и крышкой системного блока не менее 100 мм[21].

4.4 Анализ результатов

Для оценки эргономических условий работников отдела приема и размещения отеля «Nevsky Contour» был разработан сетевой график мониторинга ра-

бочего места и сетевой график устранения нарушений (параметров рабочей зоны, освещения, микроклиматических условий, конструкции стола и стула, расположения и комплектации элементов ПЭВМ)[22].

Опираясь на полученные результаты было определено, что при проведении грамотной оценки эргономических условий на рабочем месте администраторов и менеджера отеля, эргономические нарушения будут проявляться раз в 184,92 суток с вероятностью 0,95; раз в 72,99 суток с вероятностью 0,9; раз в 31,75 суток с вероятностью 0,85.

Заключение

В рамках данного дипломного проекта была проведена работа по созданию и внедрению системы информационной безопасности в отеле «Nevsky Contour».

Первоначальный анализ существующей системы информационной безопасности показал, что в ней присутствовали серьезные уязвимости и существовала высокая вероятность несанкционированной утечки конфиденциальной информации посредством :

– несанкционированный съем данных через открытые двери;

– несанкционированный съем данных через окна и мониторы компьютеров;

– перехват данных по ПЭМИН;

– утечка информации через не правильную утилизацию материальных носителей;

– несанкционированный доступ к локальной сети;

– свободный доступ во все помещения отеля, включая бумажный архив.

На основе проведенных финансовых расчетов было выявлено, что в вычислительных средствах отеля «Nevsky Contour» циркулирует информация на сумму 4 565 000 рублей.

По результатам проведенного аудита была доказана необходимость разработки и внедрения системы обеспечения безопасности.

При анализе поставщиков средств защиты информаии было выбрано соответствующее и наиболее приемлемое оборудование.

В связи с тем, что отель «Nevsky Contour» является коммерческой организацией, то основной целью деятельности является получение прибыли и предоставление своим клиентам качественных услуг. Поэтому главными критериями выбора средств защиты информации являлись функционал, а так же цена оборудования. Основываясь на этот факт, из существующего многообразия

средств защиты были приобретены следующие:

– тканевые жалюзи от компании "Жалюзи Град";

– генератор шума "ГШ-К-1800";

– доводчики дверей двух типов: MSM D 180 для входных дверей, Falcon EYE FE-B4W для межкомнатных дверей;

– защитные пленки для мониторов компьютеров компании "3М";

– уничтожитель бумаги Office Kit S 145;

– комплекты системы контроля и управления доступом;

– 18 сейфов для постояльцев модели STF-20 EA, 1 сейф для администраторов модели VALBERG AW 2714, 1 сейф с доступом только для менеджера и генерального директора VALBERG ASM;

– система резервного копирования "Pervasive backup agent";

– VPN и межсетевой экран;

– антивирус Kaspersky Endpoint Security;

– отказоустойчивые RAID-массивы с шифрованием AES.

Размещение компьютеров было изменено таким образом, что бы никому невозможно увидеть изображения на мониторах, кроме работающего за ним сотрудника.

Были определены места размещения всех средств защиты и места нахождения компьютеров. Так же была разработана система управления информационной безопасностью в отеле «Nevsky Contour».Закупка, установка и настройка средств защиты информации обойдется для отеля «Nevsky Contour» в 357 453 рублей.

В результате был разработан комплекс мер по обеспечению информационной безопасности в отеле «Nevsky Contour».

Список использованной литературы

1. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 с.
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации / В.П. Мельников, - М.: Издательский центр «Академия», 2008. - 336 с
3. Петренко С.А., Курбатов В.А. - Политики безопасности компании при работе в интернет / С.А. Курбатов - ДМК Пресс, 2011. – 396 с
4. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1./ А. М. Блинов – Изд-во СПбГУЭФ, 2010. – 96 с.
5. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2010. – 458 с.
6. Попов Л.И., Зубарев А.В. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации. «Альтпресс», 2009. -512с
7. Шапаренко Ю. М., Бескид П. П., Суходольский В. Ю. «Проектирование защищенных информационных систем. Часть 1. Конструкторское проектирование. Защита от физических полей» Учебное пособие. – СПб: изд. РГГМУ, - 2008, - с. 60.
8. «Конституция Российской Федерации» / АСТ, - 2014. – 64 с.
9. ГОСТ 15971-90 / 01.01.92
10. Ярочкин В. И. «Технические каналы утечки информации».- М., 2005
11. Максимов Ю. Н. «Защита информации в системах и средствах информатизации и связи». - СПб., 2005.
12. Государственная система стандартизации. - М. Госстанда России, 1992.
13. Дурович А.П., Копанев А.С. Маркетинг в туризме: Учебное Пособие. -Минск: Экономпресс, 1998.
14. http://www.oxpaha.ru/publisher_234_28501

15. Гмурман А.И. Информационная безопасность. М.: «БИТ-М», 2004
16. Домарев В.В. Безопасность информационных технологий. Системный подход. – К: ООО ТИД «Диасофт»,2004
17. www.citforum.ru
18. www.microsoft.com
19. www.securitylab.ru
20. Агеев А. С. «Организация работ по комплексной защите информации». - К., 2003.
21. Ярочкин В. И. «Технические каналы утечки информации».- М., 2005
22. http://engine.adland.ru
23. Батурин Ю.М., Жодзинский А.М. «Компьютерная преступность и компьютерная безопасность» - М.: Юрид. лит.,1991.
24. Домарев В.В. «Безопасность информационных технологий. Системный подход». - К.: ООО ТИД «Диасофт», 2004. - 992 с
25. Евгений Касперский «Компьютерные вирусы» - М.: 1998
26. Грибунин В.Г. Политика безопасности: разработка и реализация// «Информационная безопасность», 2005, №1.
27. Д.Ведеев «Защита данных в компьютерных сетях» - М.:1995
28. Библиотека сетевой безопасности security.tsu.ru
29. Торокин А.А. «Основы инженерно-технической защиты информации». – М.: 2007. – 345 с.
30. Халяпин Д. Б., Ярочкин В. И. «Основы защиты промышленной и коммерческой». - К.,2001.
31. Ярочкин В. И. «Технические каналы утечки информации».- М., 2005
32. Максимов Ю. Н. «Защита информации в системах и средствах информатизации и связи». - СПб., 2005.

Приложение А

Таблица возможных угроз информационной безопасности в отеле «Nevsky Contour» и мер предпринятых для их решения.

Возможные угрозы	Средства для уменьшения количества уязвимостей и снижения степени ущерба от угроз
Основные непреднамеренные искусственные угрозы	
1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.); 2) неумышленная порча носителей информации	Система резервного копирования Perva-sive backup agent ; RAID массывы с шифрованием AES.
3) заражение компьютера вирусами;	Антивирусная система Kaspersky Endpoint Security
4) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;	Утверждение инструкций по работе с конфиденциальной информацией

Продолжение таблицы возможных угроз информационной безопасности в отеле «Nevsky Contour» и мер предпринятых для их решения.

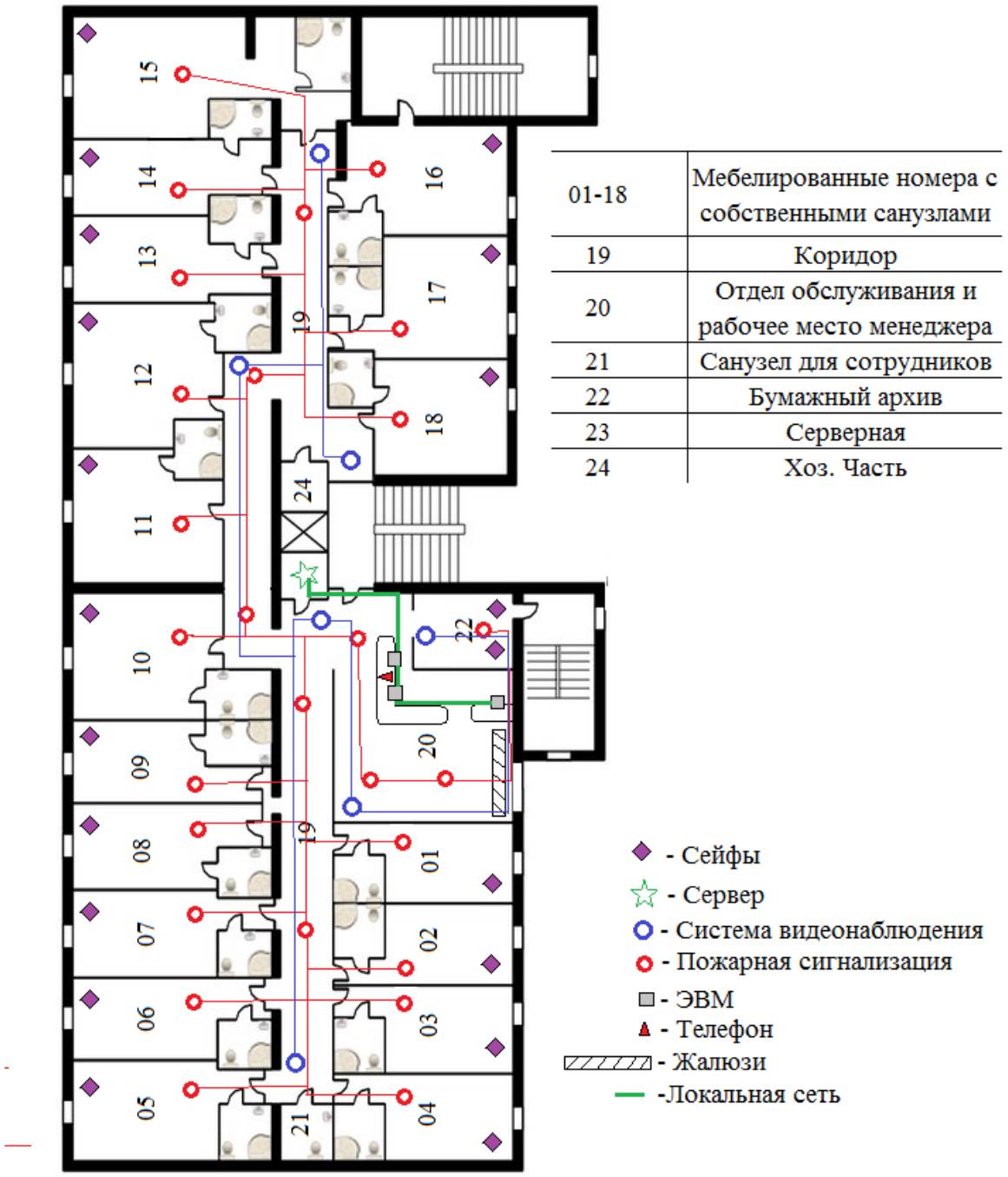
5) игнорирование организационных ограничений (установленных правил) при работе в системе;	Контроль за соблюдением правил работы с защищаемой информацией и привлечение к ответственности за ее нарушение.
Основные преднамеренные искусственные угрозы	
1) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);	Установлены источники бесперебойного питания (позволяют сохранить данные и завершить работу ПК).
2) Оптический канал утечки информации(возможность фото, видео съемки через окна, двери)	Тканевые жалюзи компании «Жалюзи Град»; Доводчики дверей моделей «MSM D 180» и « Falcon EYE FE-B4W» ; Система контроля доступа; Защитные пленки на экраны компьютеров.
3) Неправильная утилизация бумажных и магнитных носителей.	Уничтожитель бумаги « Office Kit S 145»;
4) Хранение бумажных и магнитных носителей.	Сейфы моделей « STF-20 EA», « VALBERG AW 2714» и « VALBERG ASM»;
5) Утечка информации по каналу ПЭМИН.	Генератор шума «ГШ-К-1800».

Продолжение таблицы возможных угроз информационной безопасности в отеле и мер предпринятых для их решения.

6) Несанкционированный доступ в помещения учреждения для совершения кражи или других действий в не рабочее время;	Система контроля доступа;
7) Перехват данных по сети Интернет.	Виртуальная частная сеть; Межсетевой экран.
Естественные угрозы	
1) пожары;	Установлена охранно-пожарная сигнализация Инструкция по пожарной безопасности.
2) прорыв трубы, протечка в крыше.	Инструкция по технике безопасности. Инструкция действий в нештатных ситуациях. Ознакомления персонала с ней, и распределение отвечающих при возникшей данной ситуации.

Приложение Б

План расположения всех ЭВМ и средств обеспечения информационной безопасности



01-18	Мебелированные номера с собственными санузлами
19	Коридор
20	Отдел обслуживания и рабочее место менеджера
21	Санузел для сотрудников
22	Бумажный архив
23	Серверная
24	Хоз. Часть