МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФГБОУ ВПО «Брянский государственный технический университет»

Кафедра «Экономика, организация производства, управление»

**Курсовая работа**

по дисциплине «Информационная безопасность»

на тему: «Проектирование системы информационной безопасности (на примере Службы доставки зоотоваров «Гав’с»

Выполнил:

студент гр. 13-ПИ

ФИО

Руководитель: к.т.н., доц.

ФИО

Брянск 2016

ЗАДАНИЕ

на курсовую работу по дисциплине

**"Информационная безопасность"**

**Студент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Группа**\_\_\_\_\_\_\_\_\_\_\_\_\_

**Тема**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ГРАФИК ВЫПОЛНЕНИЯ РАБОТЫ

*Название раздела: дата выполнения:*

Задание выдано \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Предварительная защита \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Защита курсового проекта \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель Демиденко А.И.

## Аннотация

Данная курсовая работа представляет собой проектирование системы информационной безопасности на выбранном нами объекте с информационной системой. В качестве такого объекта был выбран автосервис «Сенатор». Основной текст курсовой работы разделен на четыре раздела. Первый – анализ исходных данных. Здесь приводится описание организации с указанием организационно-штатной структуры с необходимыми комментариями. В дополнение составляется технический паспорт анализируемого автосервиса.

Второй раздел – расчет информационных рисков. Оценка рисков производится экспертом, в качестве которого выступает сам студент и определяет показатели. На данном этапе производится идентификация информационных активов и ресурсов. По имеющимся формулам расчета осуществляется оценка участия активов, их важности и стоимости. Далее проводится расчет стоимости информационных ресурсов и составляется оценочная матрица информационных ресурсов. Результатом анализа выступает перечень информационных ресурсов с их полной стоимостью и величиной максимального риска. Также в данном разделе производится анализ угроз и уязвимостей и оценка их риска.

Третий раздел определяет разработку мероприятий по защите информации и подбор технических средств. Здесь ведется расчет рисков по материалам анализа информации и анализа угроз безопасности информации, а затем проводится перекрестная оценка всех уязвимостей системы и указывается метод их предотвращения.

Четвертый раздел представляет собой непосредственно разработку политики информационной безопасности службы доставки зоотоваров «Гав’c».

Содержание

[Аннотация 2](#_Toc469909361)

[Введение 4](#_Toc469909362)

[1.Анализ исходных данных. 6](#_Toc469909363)

[1.1 Характеристика предприятия. 6](#_Toc469909364)

[1.2 Анализ технической службы доставки зоотоваров «Гав’с». 8](#_Toc469909365)

[2. Расчет информационных рисков 13](#_Toc469909366)

[2.1 Анализ информации, циркулирующей в организации 13](#_Toc469909367)

[2.2. Оценка угроз информационной безопасности 22](#_Toc469909368)

[3. Разработка мероприятий по защите информации и подбор технических средств защиты 27](#_Toc469909369)

[3.1.Расчет рисков 27](#_Toc469909370)

[4.Разработка политики информационной безопасности. 39](#_Toc469909371)

[Графическая часть 41](#_Toc469909372)

[Список используемой литературы 42](#_Toc469909373)

[Приложения 43](#_Toc469909374)

# Введение

На современном этапе развития нашего общества многие традиционные ресурсы человеческого прогресса постепенно утрачивают свое первоначальное значение. На смену им приходит новый ресурс, единственный продукт не убывающий, а растущий со временем, называемый информацией. Информация становится сегодня главным ресурсом научно-технического и социально-экономического развития мирового сообщества. Чем больше и быстрее внедряется качественной информации в народное хозяйство и специальные приложения, тем выше жизненный уровень народа, экономический, оборонный и политический потенциал страны.

В настоящее время хорошо налаженная распределенная сеть информационно-вычислительных комплексов способна сыграть такую же роль в общественной жизни, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые. Ярким примером этому стало развитие глобальной сети Internet. Уже принято говорить о новом витке в развитии общественной формации - информационном обществе.

**Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.**

Создание систем защиты информации связано с большим числом трудностей. Они обусловлены многими факторами: быстрым развитием технологий, что приводит к появлению новых каналов утечки информации, явно выраженным антагонизмом между злоумышленником и владельцем информации, большой зависимостью системы защиты информации от опыта специалистов, которые её обслуживают и т.д.

Целью выполнения курсовой работы является систематизация и закрепление знаний, полученных при изучении дисциплины "Информационная безопасность", выработки комплексного подхода и развитие навыков к самостоятельной работе при проектировании систем информационной безопасности предприятия (организации).

В задачи курсового проектирования входят:

1. Изучение особенностей службы доставки зоотоваров «Гав’c»

2. Анализ возможных подходов и методов решения задачи построения системы информационной безопасностислужбы доставки зоотоваров «Гав’c» и обоснование выбранного подхода.

3. Выработка навыков математического моделирования и разработки структурно - функциональных схемы моделей объектов защиты информации.

4. Получение практического опыта по построению системы информационной безопасности службы доставки зоотоваров «Гав’c»на основе теоретических разработок.

5. Развитие умения разработки необходимой документации по обеспечению информационной безопасности.

# 1.Анализ исходных данных.

## 1.1 Характеристика предприятия.

Служба доставки была создана 08 июня 2005 года с целью облегчения взаимоотношений животных с их владельцами. Главной миссией «Гав’с» является обеспечение своевременного ухода за домашними животными путем продажи и доставки зоотоваров клиентам по оптовым ценам. Заказ товаров осуществляется непосредственно через сайт службы доставки зоотоваров «Гав’c»: <http://www.gaws.ru/> (Приложение 1).

«Гав’с» имеет два направления бизнеса:

1. Продажа и доставка товаров с помощью сайта.
2. Прямая продажа товара непосредственно через магазин, расположенный по адресу г. Брянск, ул. Ростовская д.4

**К целям «Гав’с» относятся:**

1. Развитие в вышеперечисленных сферах благодаря взаимной выгоде для компании и потребителей.
2. Высокий доход путем продажи товаров по самым оптимальным ценам на сегодняшний день.
3. Увеличение количества заказов.
4. Увеличение количества поставщиков, а так же долгосрочные и надежные отношения с ними.
5. Наиболее качественно и быстро удовлетворять потребности клиентов

Среднесписочная численность персонала «Гав’с» составляет 53 человека.

Организационная структура «Гав’с» (Рис.1).

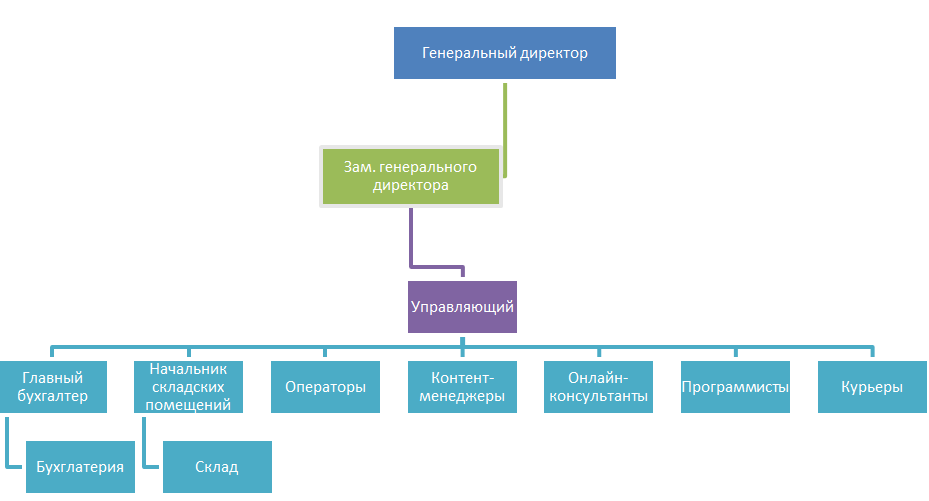


Рис.1 Организационная структура «Гав’с».

1. Генеральный директор –глава службы доставки зоотоваров «Гав’с». Функции генерального директора заключаются в общем руководстве деятельностью компании.

2. Зам. Генерального директора – лицо, имеющее все основные полномочия генерального директора во время его отсутствия.

3. Главный бухгалтер – должностное лицо предприятия, обеспечивающее организацию бухгалтерского учета, контроль и отражение на счетах бухгалтерского учета всех осуществляемых предприятием, учреждением хозяйственных' операций, предоставление оперативной информации, составление в установленные сроки бухгалтерской отчетности. Свою деятельность осуществляет на основании требований нормативных документов правительства РФ. В пределах утверждённых должностных обязанностей взаимодействует с государственными предприятиями, учреждениями и общественными организациями.

4. Начальник складских помещений – ответственное лицо за все действия, происходящие на складе, в том числе за прием товара на склад и до передачи товара курьеру.

5. Операторы – осуществляют общение с клиентом. Обязаны обговорить сумму заказов с бухгалтером, а так же направить курьера по необходимому адресу.

6. Контент-менеджеры – специалисты по созданию, распространению и курированию контента, редакторы сайтов. В обязанности контент-менеджера входит наполнение сайта текстовой, графической и другими видами информации, полезной и удобной для восприятия выбранной целевой группой (контентом).

7. Онлайн-консультанты – лица, в обязанность которых входит: консультирование клиентов по тому или иному товару, о его начилии на складе; уточнение цены на товар; подбор товара с интересующими клиента характеристиками.

8. Программисты – специалисты по программированию, задача которых обеспечивать стабильную работу сайта, корректное отображение торговых позиций, обновление дизайна.

9. Курьеры – лица, в задачу которых входит прием заказанного товара на складе «Гав’c» и доставка клиенту по его адресу в намеченные сроки.

**Услуги, предоставленные «Гав’c»:**

* Продажа зоотоваров по оптовым ценам.
* Доставка – компания «Гав’c» обладает развитой системой доставки зоотоваров как по Москве и Подмосковью, так и по многим регионом России. При заказе от 2000 рублей и более, доставка осуществляется бесплатно.
* Бесплатная консультация клиентов по выбору зоотоваров для определенных пород животных.

**«Гав’c» предлагает разнообразную продукцию для животных:**

* Корма для кошек, собак, рыб, черепах, попугаев, канареек, грызунов, лошадей;
* Посуда: кормушки, миски, поилки, бутылки, соски, контейнеры для корма;
* Вет-препараты: витамины, подкормки, средства от паразитов, вакцины, иммунные препараты, антибактериальные препараты, инсулины, кардиопрепараты, противовоспалительные препараты, противоопухолевые препараты, антиоксиданты, пробиотики, гормональные препараты, корректирующие поведение, капли ушные и глазные, мази и шампуни дерматологические, растворы и спреи, седативные препараты, оборудование и расходные материалы.
* Амуниция: намордники, поводки, ошейники, шлейки, адресники, одежда;
* Аквариумное оборудование: термооборудование, системы СО2, фильтры, помпы, насосы, осветительное оборудование;
* Шампуни, лосьоны, расчески;
* Туалеты с наполнителями;
* Домики, клетки, переноски, загоны, когтеточки;
* Игрушки для собак, кошек и птиц;
* Книги, в которых содержится подробная инструкция об уходе за теми или иными животными.

## 1.2 Анализ технической службы доставки зоотоваров «Гав’с».

Анализ технической оснащённости включает: план помещения, который представлен в графической части курсового проекта, технический паспорт помещения (табл.1).

Таблица 1

Технический паспорт службы доставки зоотоваров «Гав’с»

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Наименование объекта** | | | **Характеристики** | | | |
| Этаж (в здании 2 этажа) | | | 1-й этаж | | | |
| Наличие хранилищ бумажных документов | | | 1 | | | |
| Порядок доступа в помещения | | | Все помещения закрываются под ключ, всё ставится под охрану (сигнализацию) | | | |
| Состав технических средств | | | | | | |
| Количество и тех. характеристикисерверов | | | Количество:1;  Операционная система: WindowsServer 2008 R2 х64  Процессор: Intel® Corei5 – 2400 @ 3,1 GHz  ОЗУ: 24 гб  HDD: 4 шт по 1 TB | | | |
| Количество и характеристики АРМ | | | Количеств: 5 шт; Операционная система: Windows Server 2008 R2 х64  Процессор: Intel® Corei5 – 2400 @ 3,1 GHz  ОЗУ: 24 гб  HDD: 4 шт по 1 TB | | | |
| Количество коммутаторов ЛВС | | | | | Коммутатор управляемый: 1 шт.;  Производитель: D-Link;  Модель:DGS-1100-16;  Пропускная способность: 32 Гбит/с;  Количество портов: 16 |
| Выход в Internet | | | | |
| Тип подключения | | | | Каналы по технологии ADSL, скорость передачи до 100 Мбит/сек |
| Характеристика ПО | | | |
| Информационное ПО | | | ОС: Microsoft Windows 7 Professional;  СУБД: Microsoft SQL Server 2005 |
| Дополнительное оборудование | | | |
| Камера видеонаблюдения | | | Количество: 3шт;  Производитель: Maxi-Cam;  Модель: AHD-10D"Alfa" |
| МФУ | | | Количество: 5шт;  Производитель: Brother;  Модель: HL-2035R |
| Факсы | | | Количество: 3 шт;  Производитель: Brother;  Модель: Т-106 |
| Телефоны | | Количество: 3шт;  Производитель: Akai;  Модель: AT-A15MS | |

«Гав’с» использует несколько главных программ в своей работе: 1С Предприятие 8.3, ZOOSM, Товар-Деньги-товар.

«Товар-Деньги-Товар» — универсальная торгово-складская программа. Работает в Windows XP, Vista, 7, 8, 10 (Домашняя, Профессиональная, Корпоративная, Для образовательных учреждений).

**Преимущества программы:**

* Возможность просматривать остатки, продажи и данные о реализации на любых устройствах, подключенных к интернету, в том числе смартфонах и планшетах через сервис [ТДТ Онлайн](http://www.pvision.ru/tdt/post/183).
* Работа с кассовыми аппаратами, сканерами штрих кодов, терминалами сбора данных.
* [Автоматическое заполнение реквизитов](https://youtu.be/jLe4-di5MvA).
* [Импорт оплат](https://youtu.be/BBSYKWIuBfY) из клиент банка.
* [Выписка](https://youtu.be/r1ZcB1_1q_Q) по фирме из ЕГРЮЛ/ЕГРИП.
* Работа в многопользовательском режиме. Возможность настраивать уровни доступа прав у пользователей.
* [Выгрузка остатков](http://www.pvision.ru/tdt/post/189) в интернет магазин.
* [Импорт товаров](http://www.pvision.ru/tdt/post/207) из MS Excel.
* [Работа с комплектами](http://www.pvision.ru/tdt/post/192).

1С:Предприятие — [программный продукт](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D1%8B%D0%B9_%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82) компании «[1С»](https://ru.wikipedia.org/wiki/1%D0%A1), предназначенный для автоматизации деятельности «Гав’с». Например, «Гав’c» широко использует 1С для работы с расходными накладными (Приложение 2).

Рассмотрим работу программы ZOOSM.

ZOOSM – электронный каталог актуальных товаров, предоставляемый поставщиками и с которым работают операторы при оформлении заказа.

Данная программа активно применяется на начальных стадиях покупки и оформлении товара. ZOOSM содержит множество прайсов поставщиков, с которыми активно сотрудничает «Гав’c» и по которым операторы при оформлении заказа проверяют наличие и остатки товаров, интересующие клиентов. На данном этапе необходимо выбрать нужного поставщика товара в имеющейся группе поставщиков, так же при надобности можно сформировать общий прайс всех поставщиков с помощью двойного щелчка по названию группы (Рис.2).

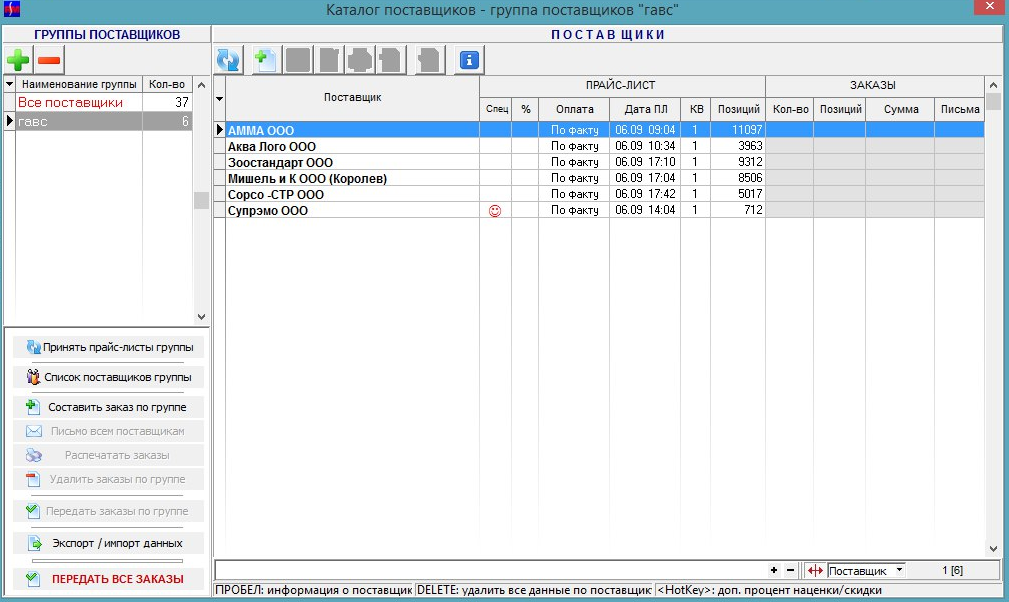


Рис. 2 Программа ZOOSM.

Далее перед нами предстает общий прайс всех поставщиков. (Рис.3) Здесь мы можем увидеть цену на товары, предоставляемые нашими поставщиками, а так же их артикул и остатки.

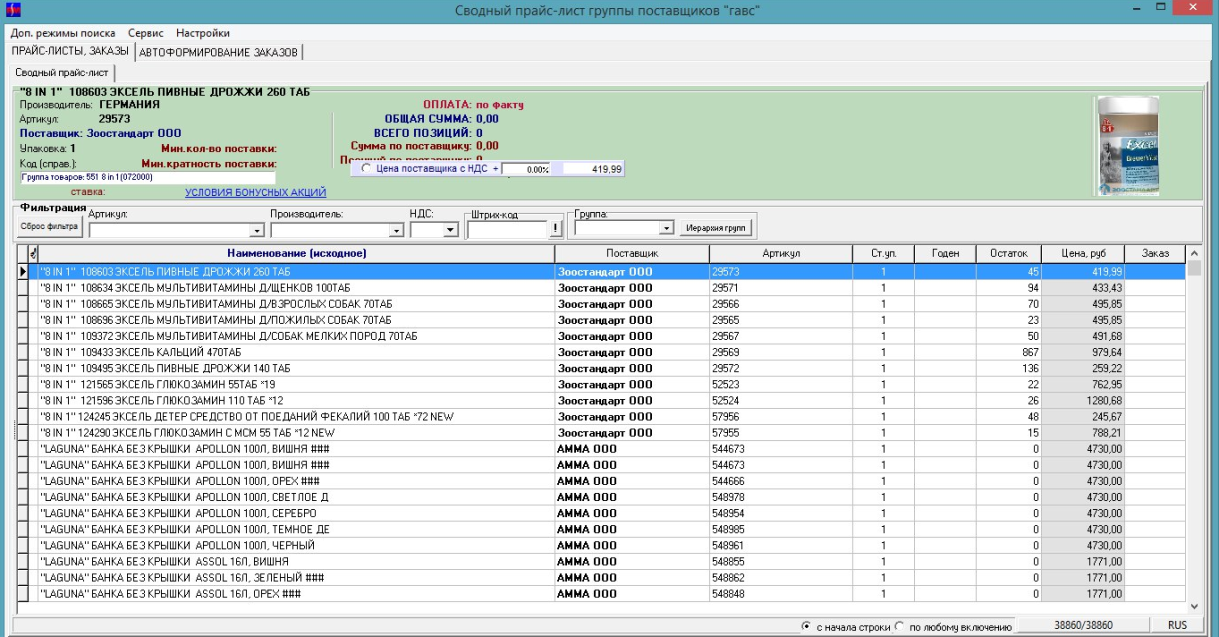


Рис.3 Обобщенный прайс

Во время оформления заказа, оператор проверяет наличие товара с помощью ввода артикула или названия товара в графу «Найти». (Рис.4)

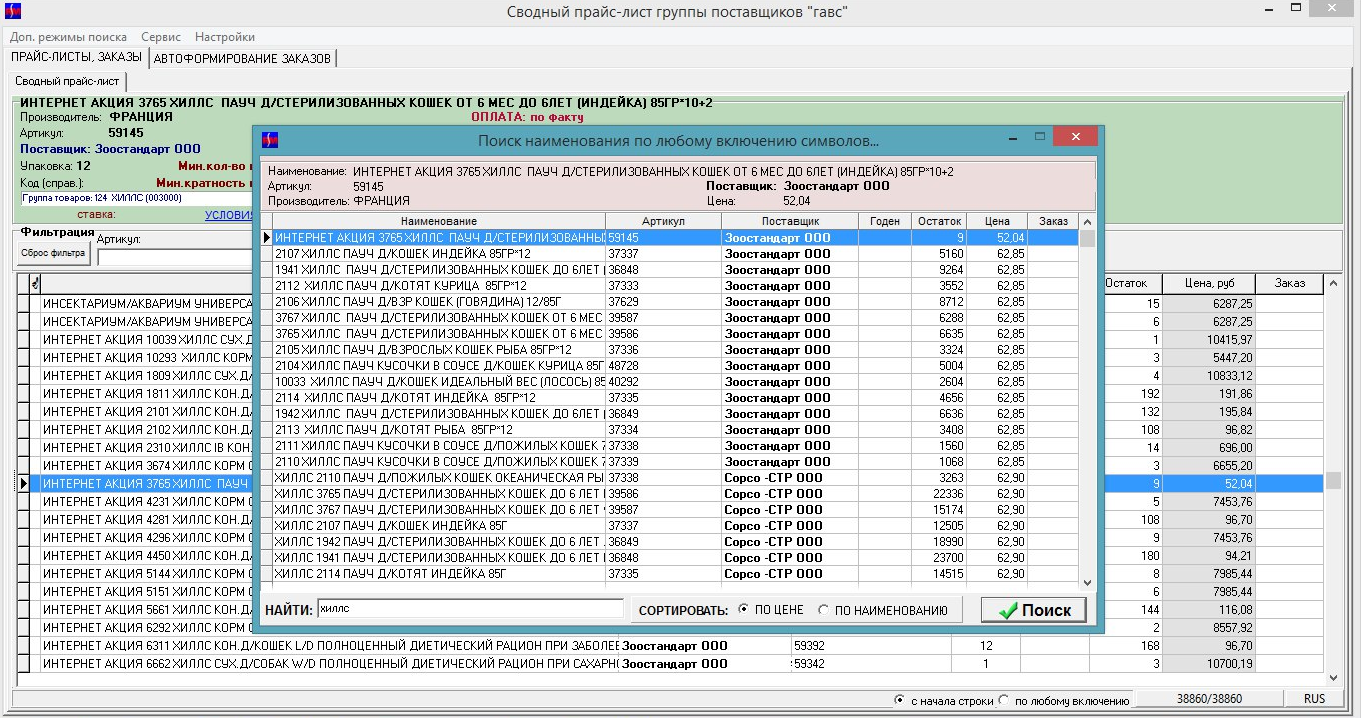


Рис.4 Проверка наличия товара в ZOOSM.

Так же, при необходимости, можно занести новых поставщиков в «Группы поставщиков» и в дальнейшем загружать и использовать их прайсы. (Рис.5)

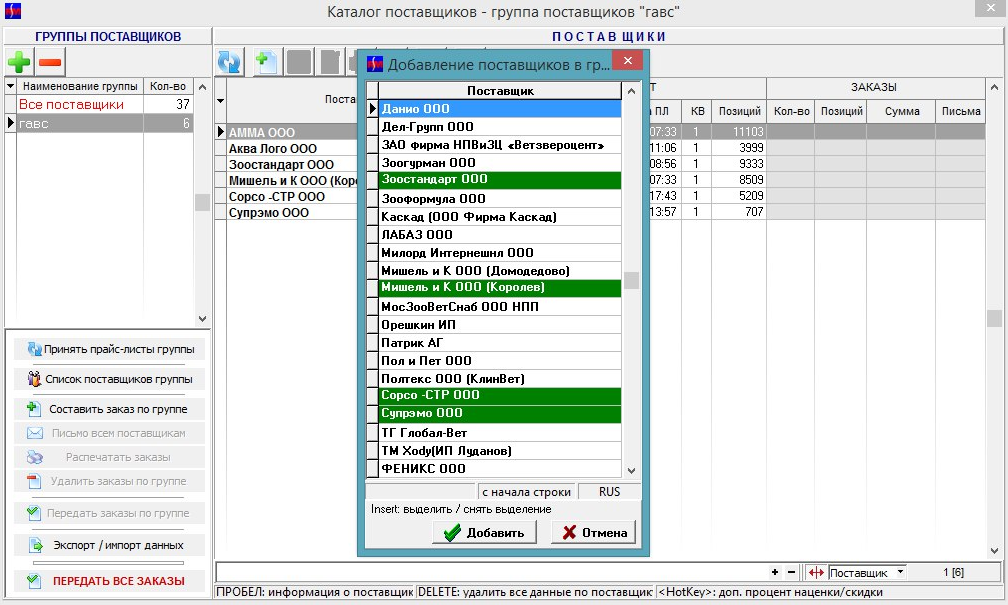


Рис.5 Добавление в группу поставщиков.

# 2. Расчет информационных рисков

## 2.1 Анализ информации, циркулирующей в организации

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации.

Его основная задача — объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. [1]

Анализ информации, циркулирующей на предприятии основывается на рассмотрении:

1. Идентификации и оценки информационных активов (ИА).
2. Идентификации и оценки информационных ресурсов (ИР).

Основной целью этапа идентификации и оценки ИА является получение количественных значений вероятного ущерба при воздействии угроз информационной безопасности и минимально допустимых значений информационных рисков. Наибольшее негативное влияние может оказать нарушение целостности, конфиденциальности и доступности информационным активам.[4]

Итак, под информационными активами организации будем понимать все ценные информационные ресурсы собственника, способные приносить ему экономическую выгоду, в которых аккумулированы знания, умения и навыки персонала, и реализованные с использованием современных информационных технологий. Иначе говоря, информационные активы необходимо рассматривать как неотделимую совокупность самих сведений, средств их обработки и персонала, имеющих к ней доступ и непосредственно их использующие. [2]

Служба доставки зоотоваров «Гав’c» обладает следующими основными информационными активами:

* Электронная информация/данные,
* Информация на бумажных носителях,
* Архивные документы (отчетность за прошлые периоды),
* Аналитические данные для высшего руководства,
* Человеческие ресурсы,
* Персональные данные,
* Физические активы (сервера, АРМ, терминалы, сетевое оборудование, мобильные устройства),
* Сервисные ресурсы (эл. почта, веб-ресурсы),
* Программное обеспечение, включая прикладные программы,
* Имидж компании.

Проведем оценку данных информационных активов:

Каждый актив, в том числе и неинформационный, оценивается по его “участию в прибыли” (Oy). Для выставления оценки необходимо определить значения лингвистических переменных:

- малая степень участия 1;

- средняя степень участия 3;

- высокая степень участия 5;

- очень большая степень участия 7.

Рассчитывается “коэффициент участия” (Ky):

,

Где i – порядковый номер актива.

Значения коэффициента участия для каждого информационного актива отдела представлены в табл.2.

Таблица 2

Расчет коэффициента участия для каждого ИА

|  |  |
| --- | --- |
| Информационный актив | Коэффициент участия (Ky) |
| Электронная информация/данные |  |
| Информация на бумажных носителях |  |
| Архивные документы (отчетность за прошлые периоды) |  |
| Аналитические данные для высшего руководства |  |
| Человеческие ресурсы |  |
| Персональные данные |  |
| Физические активы (сервера, АРМ, терминалы, сетевое оборудование, мобильные устройства) |  |
| Сервисные ресурсы (эл. почта, веб-ресурсы) |  |

*Окончание табл.2*

|  |  |
| --- | --- |
| Программное обеспечение, включая прикладные программы |  |
| Имидж компании |  |

Рассчитывается сумма участия актива в прибыли (Sy).

Чистая прибыльслужбы доставки зоотоваров «Гав’с»по данным финансовой отчетности за 2015 г. составила 2 104 000 руб.

Расчеты в пунктах 2) и 3) проводятся только для информационных ресурсов. Сведем данные в табл. 3

Таблица 3

Анализ информационных активов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п.п | Наименование актива | Оценка участия  (Оy) | Коэф. участия  (Кy) | Сумма участия, руб.  (Sy) |
| 1 | Электронная информация/данные | 7 | 0,121 | 133 584 |
| 2 | Информация на бумажных носителях | 5 | 0,085 | 93 840 |
| 3 | Архивные документы (отчетность за прошлые периоды) | 5 | 0,085 | 93 840 |
| 4 | Аналитические данные для высшего руководства | 7 | 0,121 | 133 584 |
| 5 | Человеческие ресурсы | 7 | - | - |
| 6 | Персональные данные | 3 | 0,052 | 57 408 |
| 7 | Физические активы (сервера, АРМ, терминалы, сетевое оборудование, мобильные устройства) | 5 | - | - |
| 8 | Сервисные ресурсы (эл. почта, веб-ресурсы) | 7 | - | - |
| 9 | Программное обеспечение, включая прикладные программы | 7 | - | - |
| 10 | Имидж компании | 3 | - | - |
|  | Итоговая сумма прибыли ИА (SПИА): |  |  | 512 256 |

Для оценки важности необходимо выполнить следующие расчеты:

а) определить сумму прибыли, получаемую за счет информационных активов

б) Далее следует оценить важность каждого ИА. Оценка производится экспертами аналогично оценке участия актива в прибыли. В результате каждому активу должен быть присвоен “коэффициент важности”, который должен удовлетворять двум условиям:

,

Гдеn – порядковый номер информационного актива.

Расчет стоимости каждого ИА производится, как произведение прибыльной стоимости информации и коэффициента важности.

Для программного обеспечения:

руб.

Аналогично рассчитаем стоимость для остальных ИА.

Стоимость информационного актива определяет минимально допустимое значением информационных рисков для него.

Сведем полученные данные в табл. 4.

Таблица 4

Анализ стоимости информационных активов

|  |  |  |  |
| --- | --- | --- | --- |
| №  п.п | Наименование актива | Коэф.  Важности  (К) | Стоимость актива  (SИА) |
| 1 | Электронная информация/данные | 0,12 | 61 471 |
| 2 | Информация на бумажных носителях | 0,08 | 40 980 |
| 3 | Архивные документы (отчетность за прошлые периоды) | 0,10 | 51 225 |
| 4 | Аналитические данные для высшего руководства | 0,12 | 61 471 |
| 5 | Человеческие ресурсы | 0,12 | 61 471 |
| 6 | Персональные данные | 0,05 | 25 613 |
| 7 | Физические активы (сервера, АРМ, терминалы, сетевое оборудование, мобильные устройства) | 0,10 | 51 225 |
| 8 | Сервисные ресурсы (эл. почта, веб-ресурсы) | 0,13 | 66 593 |
| 9 | Программное обеспечение, включая прикладные программы | 0,11 | 56 348 |
| 10 | Имидж компании | 0,07 | 35 587 |

В отделе продаж предприятия работают 6 сотрудников.

Необходимо рассчитать стоимость информационных ресурсов, необходимых для формирования соответствующих документов:

1. Бумажные документы (договора, акты, деловые письма, протоколы совещаний, методики обучения персонала, система организации труда);
2. Электронные документы, находящиеся на АРМ работников отдела(документы, поступающие из подконтрольных отделов: бухгалтерия, материально-техническая служба, техническая документация, инструкции по эксплуатации терминалов);
3. Аналитические отчеты;
4. Архивы документов по работе автосервиса (отчетность за прошлые периоды);
5. Коммуникационный сервер, использующийся для принятия и передачи электронных сообщений (электронная почта, мгновенные сообщения в коммуникаторе);
6. Файловый сервер, использующийся как сетевой ресурс общего доступа сотрудников.

Стоимость ИР определяется как сумма всех фактических расходов на приобретение, приведение и поддержании их в состоянии, в пригодном для использования в запланированных целях. Расчет стоимости информационных ресурсов произведен в таблице 5.

Таблица 5

Расчет стоимости информационных ресурсов

|  |  |  |  |
| --- | --- | --- | --- |
| №ИР | Наименование параметра | Единица измерения | Значение |
| 1 | Заработная плата сотрудникам за месяц | Руб. | 90000 |
| Расход бумаги (затраты на бумагу) | Руб. | 2500 |
| Расход тонера | Руб. | 500 |
| Итого (SИРз1): | Руб. | 93000 |
| 2 | Обслуживание ЭВМ | Руб. | 16000 |
| Заработная плата сотрудникам за месяц |  | 90000 |
| Оплата Internet | Руб. | 1500 |
| Обслуживание ИС | Руб. | 5000 |
| Прочие расходы | Руб. | 2000 |
| Итого (SИРз2): | Руб. | 98500 |
| 3 | Заработная плата сотрудникам за месяц | Руб. | 90000 |
| Расход бумаги | Руб. | 2000 |
| Расход тонера | Руб. | 500 |
| Прочие расходы | Руб. | 1000 |
| Итого (SИРз3): |  | 93500 |
| 4\* | Расходы на хранение(SИРз4): | Руб. | 4500 |
| 5 | Обслуживание ЭВМ | Руб. | 7500 |
| Прочие расходы | Руб. | 1500 |
| Итого (SИРз5): | Руб. | 9000 |
| 6 | Обслуживание ЭВМ | Руб. | 40000 |
| Прочие расходы | Руб. | 300 |
| Итого (SИРз6): | Руб. | 43000 |

\* – для ресурса 4 характерны те же расходы, что и для ресурса 1, но потраченные в прошлые периоды. В текущем периоде, характерны только расходы на хранение.

Под стоимостью информации содержащееся в ИР понимается часть стоимости ИА. ИР является материальным воплощением ИА. Причем каждый актив может быть реализован несколькими ресурсами. В то же время каждый ресурс может содержать информацию нескольких активов. Поэтому в полную стоимость ИР необходимо включить часть стоимости актива, пропорциональную количеству информации этого актива в ресурсе.

Для этого определим перечень информационных ресурсов, которые реализуют активы:

Данные на бумажных носителях:

* договора (трудовые договора, договора на оказание услуг, договора сотрудничества и т.д.),
* акты о приемке выполненных работ и др.,
* деловые письма,
* протоколы совещаний,
* программы обучение персонала;

Электронные данные:

* бухгалтерская отчетность,
* планово-экономическая информация,
* информация об объемах выполненных работ;

Архивные документы:

* информация о сделках за прошлые периоды;
* документы о работе с поставщиками,
* отчетность и результаты работы автосервиса за предыдущие периоды;

Аналитическая отчетность, в этот актив входят следующие ресурсы:

* отчет по проведенным работам,
* отчет о персонале,
* отчет по оборудованию,
* отчет по затратам;

Персональные данные, для этого актива соответствуют следующие ресурсы:

* финансовые ведомости,
* сведения о клиентах,
* банковские реквизиты для осуществления расчетов с клиентами.

Составим матрицу информационных ресурсов. Нулевое значение коэффициента означает, что данный ресурс не участвует в реализации данного актива. Сумма значений коэффициентов в столбцах матрицы должна быть равна 1 (табл. 6).

Таблица 6

Матрица информационных ресурсов

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п.п. | Активы  Ресурсы | | Актив 1 | | Актив 2 | Актив 3 | Актив 4 | Актив 5 |
| 1 | Договора | | 0,2 | | 0,1 | 0 | 0 | 0 |
| 2 | Акты | | 0,1 | | 0 | 0 | 0 | 0 |
| 3 | Деловые письма | | 0 | | 0 | 0 | 0 | 0,1 |
| 4 | Протоколы совещаний | | 0,1 | | 0,1 | 0 | 0 | 0 |
| 5 | Программы обучения персонала; | | 0 | | 0,1 | 0 | 0 | 0,1 |
| 6 | Бухгалтерская отчетность | | 0,2 | | 0,2 | 0,1 | 0 | 0 |
| 7 | Планово-экономическая информация | 0,1 | | 0,2 | | 0 | 0 | 0 |
| 8 | Данные отдела продаж | 0 | | 0,3 | | 0 | 0 | 0 |
| 9 | Информация о сделках за прошлые периоды | 0 | | 0 | | 0,2 | 0 | 0 |
| 10 | Документы о работе с поставщиками | 0,1 | | 0 | | 0,2 | 0 | 0 |
| 11 | Отчетность и результаты работы автосервиса за предыдущие периоды | 0 | | 0 | | 0,4 | 0 | 0 |
| 12 | Отчет о персонале | 0 | | 0 | | 0 | 0,2 | 0 |
| 13 | Отчет по проведению работ (услуг) | 0 | | 0 | | 0 | 0,4 | 0 |
| 14 | Отчет по затратам по видам | 0 | | 0 | | 0 | 0,3 | 0 |
| 15 | Отчет по оборудованию | 0 | | 0 | | 0 | 0,1 | 0 |
| 16 | Финансовые ведомости | 0,1 | | 0 | | 0 | 0, | 0,2 |
| 17 | Сведения о клиентах | 0 | | 0 | | 0,1 | 0 | 0,4 |
| 18 | Банковские реквизиты для осуществления расчетов с клиентами | 0,1 | | 0 | | 0 | 0 | 0,2 |
| Итого: |  | 1 | | 1 | | 1 | 1 | 1 |

Для определения части стоимости актива, входящую в ресурс, необходимо стоимость актива (SИА) умножить на коэффициент.

Определение стоимости части актива представлено в табл. 7.

Таблица 7

Определение стоимости части актива

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п.п. | Активы  Ресурсы | Актив 1 | | Актив 2 | Актив 3 | Актив 4 | Актив 5 | ,  Руб. |
| 1 | Договора | 628812,8 | | 471609,6 | 0 | 0 | 0 | 1100422,4 |
| 2 | Акты | 314406,4 | | 0 | 0 | 0 | 0 | 314406,4 |
| 3 | Деловые письма | 0 | | 0 | 0 | 0 | 196504 | 196504 |
| 4 | Протоколы совещаний | 314406,4 | | 471609,6 | 0 | 0 |  | 786016 |
| 5 | Программы обучения персонала; | | 0 | 471609,6 | 0 | 0 | 196504 | 668113,6 |
| 6 | Бухгалтерская отчетность | | 628812,8 | 943219,2 | 393008 | 0 | 0 | 1965040 |
| 7 | Планово-экономическая информация | | 314406,4 | 943219,2 | 0 | 0 | 0 | 1257625,6 |
| 8 | Данные отдела продаж | | 0 | 1414828,8 | 0 | 0 | 0 | 1414828,8 |
| 9 | Информация о сделках за прошлые периоды | | 0 | 0 | 786016 | 0 | 0 | 786016 |
| 10 | Документы о работе с поставщиками | | 314406,4 | 0 | 786016 | 0 | 0 | 1100422,4 |
| 11 | Отчетность и результаты работы предприятия за предыдущие периоды | | 0 | 0 | 1572032 | 0 | 0 | 1572032 |
| 12 | Отчет о персонале | | 0 | 0 | 0 | 943219,2 | 0 | 943219,2 |
| 13 | Отчет по проведению работ (услуг) | | 0 | 0 | 0 | 1886438,4 | 0 | 1886438,4 |
| 14 | Отчет по затратам по видам | | 0 | 0 | 0 | 1414828,8 | 0 | 1414828,8 |
| 15 | Отчет по оборудованию | | 0 | 0 | 0 | 471609,6 | 0 | 471609,6 |
| 16 | Финансовые ведомости | | 314406,4 | 0 | 0 | 0 | 393008 | 707414,4 |
| 17 | Сведения о клиентах | | 0 | 0 | 393008 | 0 | 786016 | 1179024 |
| 18 | Банковские реквизиты для осуществления расчетов с клиентами | | 314406,4 | 0 | 0 | 0 | 393008 | 707414,4 |
| Итого: | | | | | | | | 18471376 |

Стоимость информации ИР (SИРа) определяется, как сумма частей стоимости активов, которые он реализует. Полная стоимость ИР (SИР) слагается из суммы затрат на него (SИРз) и стоимости информации (SИРа), т.е.

SИР =SИРз + SИРа

Эта стоимость является величиной потерь при воздействии УБИ. Стоимость информации, содержащейся в информационном ресурсе (SИРа), в свою очередь, является минимально допустимым значением риска для данного ИР.

Рассчитаем стоимость такого ресурса как данные на бумажных носителях:

Рассчитаем стоимость электронных данных:

Рассчитаем стоимость документов, хранящихся в архивах:

Рассчитаем стоимость такого ресурса как аналитическая отчетность:

Рассчитаем стоимость такого ресурса как персональные данные:

Сведем полученные данные в таблицу 8, стоимость информационных ресурсов (табл.7) является максимальной величиной риска.

Результатом анализа информации является перечень информационных ресурсов с полной стоимостью и величиной максимального риска (табл. 8).

Таблица 8

Анализ информации защищаемого объекта

|  |  |  |  |
| --- | --- | --- | --- |
| № п.п. | Наименование ресурса | Полная стоимость ресурса | Максимальный риск |
| 1 | Данные на бумажных носителях | 3158462,4 | 3 065 462,4 |
| 2 | Электронные данные | 4735944,4 | 4 637 444,4 |
| 3 | Аналитические отчеты | 4809596 | 4 716 096 |
| 4 | Архивные документы |  | 3458470,4 |
| 5 | Персональные данные | 2692358,8 | 2593858,8 |

Т.о., в результате проведенного анализа наибольшим риском обладают электронные данные. Наименьшей степенью риска –персональные данные.

## 

## 2.2. Оценка угроз информационной безопасности

Анализ угроз информационной безопасности состоит из двух частей:

1. Анализ угроз безопасности информации(УБИ).
2. Анализ уязвимостей.

Трудности при определении значения вероятности воздействия угроз определяются тем, что УБИ – это потенциальная опасность. Т.е. объективные параметры, по которым можно оценить вероятность фактически отсутствуют. В этом случае существует только один метод – метод экспертных оценок.

Для оценки угроз по степени их опасности воспользуемся лингвистическими переменными:

– не опасно 0;

– опасно 2;

– очень опасно 4.

**I. Угрозы физической целостности, логической структуры и содержания информационных ресурсов:**

1. Сбой, отказы в работе аппаратуры; (2)

2. Ошибки в работе ПО (недокументированные возможности); (2)

3. Воздействие вредоносного ПО (вирусов); (4)

4. Стихийные бедствия и техногенные катастрофы (пожар, разрушение здания, затопление помещения); (2)

5. Ошибки персонала, вследствие недостаточной квалификации;(2)

**II. Угрозы целостности информации:**

1. Нарушение целостности со стороны персонала: ввод неверных данных, несанкционированная модификация информации, кража информации, дублирование данных; (4)
2. Потеря информации на жестких носителях; (4)
3. Угрозы целостности баз данных; (4)
4. Угрозы целостности программных механизмов работы предприятия. (2)

**II. Угрозы конфиденциальности:**

* Несанкционированный доступ к традиционным (бумажным) информационным ресурсам в помещении офиса. (2)
* Несанкционированное ознакомление с информацией путём подглядывания, подслушивания. (2)
* Несанкционированный доступ к электронным информационным ресурсам вследствие целенаправленной атаки на ИС. (4)
* Несанкционированное ознакомление с информацией при её передаче по техническим каналам связи. (4)

Воспользуемся простейшим методом оценки угроз и определим список УБИ для каждого ИА. Затем произведем оценку угроз по степени их опасности.

В итоге высчитаем оценку реальности реализации угрозы, исходя из трех параметров:

1. Ps – пространственный фактор, т.е. вероятность того, что уязвимость реализуется в том месте, где находится информация.

2. Pt – временной фактор, т.е. вероятность того, что уязвимость реализуется в тот момент, когда информация существует.

3. Pp– энергетический фактор, т.е. вероятность того, что энергии для выполнения уязвимости будет достаточно.

Итоговая оценка вычисляется прямым произведением величины вероятности каждого фактора, т.е.

Таким образом, при невыполнении хотя бы одного из прямых факторов (P = 0) уязвимость можно считать устраненной.

Величина вероятности выполнения прямых факторов зависит от косвенных. К ним можно отнести: надежность работы аппаратуры и программного обеспечения, квалификацию персонала, влияние внешней среды и т.д.Оценка угроз безопасности предприятия представлена в табл. 9.

Таким образом, была проведена оценка угроз информационной безопасности отдела, в результате которой определены основные потенциально опасные события или явления, а также рассчитана вероятность их наступления.

Таблица 9

Оценка угроз безопасности

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Узел информационной системы | Выявленная угроза БИ | | Оценка риска | |
| Угроза | Уязвимость | Ps =  Pt=  Pp = | Итоговая  оценка, P |
| 1 | Рабочее место сотрудника | Разглашение информации | Халатность или злоумышленные действия сотрудников (передача или утрата атрибутов разграничения доступа) | Ps=0,68  Pt =1  Pp =1 | 0,68 |
| Несанкционированное копирование информации на внешние носители | Отсутствие разграничений прав доступа различных групп пользователей | Ps = 1  Pt=0,42  Pp =1 | 0,42 |
| Нарушение целостности со стороны персонала | Ошибки пользователей, повлекшие удаление или искажение информации. | Ps=0,42  Pt =1  Pp =1 | 0,42 |

*Продолжение табл. 9*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | Нарушение целостности со стороны персонала | Невысокий уровень владения установленным на предприятии ПО (или же полное отсутствие навыков работы с ним) | Ps=0,37  Pt = 1  Pp= 1 | 0,37 |
|  |  |  | Большая вероятность заражения АРМ вирусами ввиду отсутствия ограничения доступа пользователей к сети интернет | Ps=0,62  Pt = 1  Pp= 1 | 0,62 |
|  |  | Сбои, отказы в работе аппаратного и программного обеспечение | Ошибочные действия персонала, в результате которых происходят сбои работы сетевого программного обеспечения | Ps =0,4  Pt = 0,4  Pp =1 | 0,16 |
| 2 | Серверы | Перехват данных, НСД | Недостаточное количество средств программной и аппаратной защиты информации | Ps = 1  Pt =0,8  Pp =0,7 | 0,56 |
|  |  |  | Отсутствие видеонаблюдения в серверной комнате | Ps = 0,35  Pt =1  Pp =1 | 0,35 |
|  |  | Угроза нарушения целостности со стороны персонала | Отсутствие разграничений прав доступа сотрудников организации ко всей имеющейся на сервере информации | Ps =1  Pt=0,76  Pp =1 | 0,76 |
|  |  | Сбои в работе программного и аппаратного обеспечения | Выход системы из штатного режима эксплуатации в случае превышения расчетного числа запросов пользователями | Ps =0,4  Pt = 0,4  Pp =0,3 | 0,048 |
|  |  |  | Перебоев системах электропитания, кондиционирования серверной комнаты | Ps =1  Pt = 0,5  Pp =0,7 | 0,35 |

*Окончание табл. 9*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | Потеря данных | Сбои в работе активного сетевого оборудования | Ps =0,6  Pt = 0,4  Pp =0,3 | 0,072 |
| 3 | Места хранения бумажных документов и электронных носителей. | Несанкционированный доступ к бумажным ресурсам, находящимся в архивах и хранилищах | Отсутствие системы контроля доступа сотрудников к архивам | Ps =1  Pt = 0,8  Pp =0,8 | 0,64 |
|  |  | Утеря документов | Невнимательность сотрудников и обслуживающего персонала (человеческий фактор) | Ps =1  Pt = 0,7  Pp =1 | 0,7 |

# 3. Разработка мероприятий по защите информации и подбор технических средств защиты

## 3.1.Расчет рисков

В настоящее время одним из важнейших условий обеспечения безопасности любого предприятия, ориентированного на получение стабильных прибылей и эффективную работу, является разработка программы управления рисками предприятия. Ее целями и задачами являются:

а) идентификация, анализ, определение количества и оценка всех рисков предприятия, сопутствующих его операционной, финансовой и стратегической деятельности. Такие риски состоят из традиционных страховых рисков, а также финансовых, товарных, юридических, экологических и других рисков, которые угрожают стабильности доходов (например, введение торгового эмбарго, или потеря престижа торговой марки);

б) выработка конкретных рекомендаций по борьбе с выявленными рисками;

в) контроль за ходом выполнения рекомендованных мероприятий и внесение необходимых корректив.

Обеспечение информационной безопасности — одна из главных задач современного предприятия. Угрозу могут представлять не только технические сбои, но и несогласованность данных в различных учетных системах, которая встречается едва ли не у каждой второй компании, а также неограниченный доступ сотрудников к информации.

Информационные риски — это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий. Иными словами, IT-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи. [7]

Информационный риск вызывается внутренними или внешними причинами. Если причины информационного риска порождаются внутри предприятия, то такой риск относится к внутренним. Внешним информационным риском считается риск, причины возникновения которого находятся за пределами предприятия.

Информационные риски можно разделить на две категории:

-риски, вызванные утечкой информации и использованием ее конкурентами или сотрудниками в целях, которые могут повредить бизнесу;

-риски технических сбоев работы каналов передачи информации, которые могут привести к убыткам.

Для разработки комплекса мероприятий по защите информации необходимо провести анализ информационных рисков, который включает:

1. Расчета рисков.

2. Перекрёстного анализа.

Расчет рисков ведётся по материалам анализа информации и анализа УБИ. (табл.10).

Таблица 10

Расчет информационных рисков

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № ИР | Наименование угрозы | Наименование уязвимости | Риск | Макс. возможный риск |
| 1 | Нарушение целостности со стороны персонала;  Перехват данных, НСД | Отсутствие разграничений прав доступа различных групп пользователей;  Недостаточное количество средств программной и аппаратной защиты  информации; | 0,56 | 1100422,4 |
| 2 | Нарушение целостности со стороны персонала;  Несанкционированное копирование информации на внешние носители  Перехват данных, НСД | Отсутствие разграничений прав доступа различных групп пользователей;  Недостаточное количество средств программной и аппаратной защиты информации | 0,42 | 314406,4 |

*Продолжение табл.10*

| 3 | Нарушение целостности со стороны персонала;  Несанкционированное копирование информации на внешние носители | Отсутствие разграничений прав доступа различных групп пользователей;  Ошибки пользователей, повлекшие удаление или искажение информации.  Недостаточное количество средств программной и аппаратной защиты информации; | 0,42 | 196504 |
| --- | --- | --- | --- | --- |
| 4 | Несанкционированное копирование информации на внешние носители  Перехват данных, НСД | Отсутствие разграничений прав доступа различных групп пользователей;  Недостаточное количество средств программной и аппаратной защиты информации | 0,42 | 786016 |
| 5 | Несанкционированное копирование информации на внешние носители | Отсутствие разграничений прав доступа различных групп пользователей | 0,51 | 668113,6 |
| 6 | Сбои, отказы в работе аппаратного и программного обеспечение;  Нарушение целостности со стороны персонала | Ошибочные действия персонала, в результате которых происходят сбои работы сетевого программного обеспечения;  Невысокий уровень владения установленным на предприятии ПО;  Перебоев системахэлектропитания, кондиционирования серверной комнаты | 0,27 | 1965040 |

*Продолжение табл. 10*

| 7 | Несанкционированное копирование информации на внешние носители;  Угроза нарушения целостности со стороны персонала; | Отсутствие разграничений прав доступа различных групп пользователей;  Недостаточное количество средств программной и аппаратной защиты информации;  Ошибки пользователей, повлекшие удаление или искажение информации. | 0,32 | 1257625,6 |
| --- | --- | --- | --- | --- |
| 8 | Потеря данных;  Угроза нарушения целостности со стороны персонала  Разглашение информации | Сбои в работе активного сетевого оборудования;  Перебоев системахэлектропитания, кондиционирования серверной комнаты;  Отсутствие разграничений прав доступа сотрудников организации ко всей имеющейся на сервере информации  Халатность или злоумышленные действия сотрудников; | 0,28 | 1414828,8 |
| 9 | Угроза нарушения целостности со стороны персонала;  Утеря документов | Отсутствие разграничений прав доступа сотрудников организации ко всей имеющейся на сервере информации;  Невнимательность сотрудников и обслуживающего персонала (человеческий фактор) | 0,32 | 786016 |
| 10 | Угроза нарушения целостности со стороны персонала | Отсутствие разграничений прав доступа сотрудников организации ко всей имеющейся на сервере информации | 0,37 | 1100422,4 |

*Продолжение табл.10*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11 | Сбои, отказы в работе аппаратного и программного обеспечение; | Ошибочные действия персонала, в результате которых происходят сбои работы сетевого программного обеспечения; | 0,16 | 1572032 |
| 12 | Нарушение целостности со стороны персонала;  Сбои в работе программного и аппаратного обеспечения | Невысокий уровень владения установленным на предприятии ПО (или же полное отсутствие навыков работы с ним);  Выход системы из штатного режима эксплуатации в случае превышения расчетного числа запросов пользователями;  Перебоивсистемахэлектропитания, кондиционирования серверной комнаты; | 0,048 | 943219,2 |
| 13 | Несанкционированное ознакомление с информацией, копирование информации на внешние носители  Сбои в работе программного и аппаратного обеспечения | Отсутствие разграничений прав доступа различных групп пользователей  Выход системы из штатного режима эксплуатации в случае превышения расчетного числа запросов пользователями | 0,28 | 1886438,4 |
| 14 | Несанкционированное ознакомление с информацией, копирование информации на внешние носители  Сбои в работе программного и аппаратного обеспечения | Отсутствие разграничений прав доступа различных групп пользователей  Выход системы из штатного режима эксплуатации в случае превышения расчетного числа запросов пользователями | 0,28 | 1414828,8 |

*Окончание табл.10*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 15 | Несанкционированное ознакомление с информацией, копирование информации на внешние носители  Сбои в работе программного и аппаратного обеспечения | Отсутствие разграничений прав доступа различных групп пользователей  Выход системы из штатного режима эксплуатации в случае превышения расчетного числа запросов пользователями | 0,28 | 471609,6 |
| 16 | Несанкционированный доступ к бумажным ресурсам, находящимся в архивах и хранилищах  Разглашение информации | Отсутствие системы контроля доступа сотрудников к архивам;  Халатность или злоумышленные действия сотрудников (передача или утрата атрибутов разграничения доступа) | 0,18 | 707414,4 |
| 17 | Угроза нарушения целостности со стороны персонала | Большая вероятность заражения АРМ вирусами ввиду отсутствия ограничения доступа пользователей к сети Интернет | 0,37 | 1179024 |
| 18 | Перехват данных, НСД | Недостаточное количество средств программной и аппаратной защиты информации | 0,56 | 707414,4 |

Для разработки организационно-технических мероприятий необходимо провести перекрёстную оценку всех уязвимостей системы. Результаты оценки должныпредставлены в табл. 11.

Таблица 11

Совокупная оценка уязвимости информационной системы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Уязвимость | № ИР | Метод предотвращения | Снижаемый  показатель  (Ps, Pt, Pp) |
|  | Отсутствие разграничений прав доступа различных групп пользователей; | 1-16 | Разработка и доведение до сотрудников политики безопасности, использование программно-аппаратных средств разграничения доступа.  Регулярное выполнение процедуры резервного копирования информации ограниченного доступа. | Ps≈0,27  Pt≈0,11 |
|  | Большая вероятность заражения АРМ вирусами ввиду отсутствия ограничения доступа пользователей к сети Интернет | 4,17 | Использование антивирусного ПО, обеспечивающего более высокий уровень защиты.  Централизованная поддержка и обновление антивирусного программного обеспечения. Систематическая проверка АРМ на наличие вредоносных программ. | Ps≈0,13  Pt≈0,5  Pp≈0,4 |

*Продолжение табл. 11*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Недостаточное количество средств программной и аппаратной защиты информации; | 1,2,3,4,7 | Развертывание системы обнаружения (предотвращения) вторжений, контроль защищенности ЛВС от атак (использование сканеров уязвимостей).  Передача данных в зашифрованном виде, использование VPN-туннелей, ЭЦП. | Ps≈0,51  Pt≈0,23  Pp≈0,33 |
|  | Ошибки пользователей, повлекшие удаление или искажение информации. | 6, 7, 12-14 | Обучение пользователей регламентам работы с АРМ.  Регулярное выполнение процедуры резервного копирования информации ограниченного доступа;  Внедрение системы контроля действий пользователя.  Использование инструментов восстановлении потерянных файлов в результате программных сбоев, файлов, удаленных с жесткого диска | Ps≈0,13  Pt≈0,53 |
|  | Невысокий уровень владения установленным на предприятии ПО | 6,12,14 | Регулярное обучения любого количества сотрудников навыкам работы с установленным вне зависимости от их территориального местонахождения и без отрыва от рабочего процесса,  Внедрение системы контроля действий пользователя. | Ps≈0,21  Pt≈0,23 |

*Окончание табл. 11*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Перебои в системах электропитания, кондиционирования серверной комнаты | 6,8,12,13,15 | Использование источников бесперебойного питания.  Установка датчиков регистрации признаков аварии или стихийного бедствия (дыма, наличия открытого огня). | Ps≈0,31  Pt≈0,13  Pp≈0,27 |
|  | Сбои в работе активного сетевого оборудования; | 8, 9 | Регулярная проверка технического состояния и ремонт оборудования | Ps≈0,02  Pt≈0,12 |
|  | Невнимательность, халатность или злоумышленные действия сотрудников | 8, 9, 12-16 | Регулярное повышение уровня знаний сотрудников компании в области ИБ, создание корпоративной культуры в области ИБ и атмосферы информационной безопасности. | Ps≈0,21  Pt≈0,5  Pp≈0,26 |
|  | Выход системы из штатного режима эксплуатации в случае превышения расчетного числа запросов пользователями; | 12-16 | Установка межсетевого экрана, ограничение доступа к настройкам маршрутизатора по ip-адресу, установка стойкого пароля на доступ к настройкам маршрутизатора. | Ps≈0,18  Pt≈0,14 |
|  | Отсутствие системы контроля доступа сотрудников к архивам | 17,18 | Использование охранной сигнализации в защищаемом помещении.  Регулярный контроль состояния защищаемого помещения. | Ps≈0,1  Pt≈0,08 |

Программно-технические меры защиты информации - это совокупность аппаратных и программных средств и мероприятий по их использованию в интересах защиты конфиденциальности информации.[4]

**Программно-аппаратные средства защиты информации:**

1.Антивируснаясистема*Касперского для WindowsServersEnterpriseEdition*.Обеспечивает:

* Постоянная антивирусная защита и проверка по требованию

Приложение проверяет все запускаемые и модифицируемые файлы, проводит лечение или удаление зараженных объектов, а также помещает подозрительные объекты в карантин для дальнейшего анализа. Приложение также проводит антивирусную проверку заданных областей по запросу администратора.

* Проактивная защита от вредоносного ПО

Современная система антивирусной защиты позволяет обнаружить вредоносные программы, даже если они еще не внесены в антивирусные базы.

* Гибкие настройки проверки

АнтивирусКасперскогодля Windows Servers Enterprise Edition позволяет:

* + настраивать глубину проверки;
  + указывать, какие типы файлов следует проверять всегда;
  + задавать действия программы при обнаружении подозрительных и зараженных объектов в зависимости от типов угроз.
* Оптимизированная производительность

Фирменные технологии «Лаборатории Касперского» iSwift и iChecker позволяют экономить время и повышать скорость работы приложения, т.к. проверка выполняется только для новых и измененных файлов.

* Проверка критических областей системы

Отдельная задача позволяет проверять области ОС, наиболее подверженные заражению — например, объекты автозапуска и оперативную память.

* Защита терминальных серверов

Программа защищает терминальные серверы MicrosoftTerminalServices и CitrixXenApp, обеспечивает защиту конечных пользователей, работающих в режиме публикации рабочего стола и приложений,

* + информирует конечных пользователей о событиях средствами службы терминалов и обеспечивает аудит всех действий,
  + производимых над файлами и скриптами.
* Поддержка виртуализированных сред

С сертификатом VMwareReady и проверенной поддержкой Hyper-V антивирус Касперского для WindowsServerEnterpriseEdition обеспечивает надежную защиту виртуализированной инфраструктуры.

* Поддержка кластеров

Созданное для работы на кластерах серверов со сложной архитектурой, приложение защищает локальные диски сервера и общие диски кластера, которыми в текущий момент владеет защищаемый узел.

2.Сканер уязвимостей *XSpider* - сетевой сканер уязвимостей проверяющий все возможные уязвимости независимо от программной и аппаратной платформы узлов.

Универсальный сетевой сканер уязвимостей XSpider способен проводить тестирование уязвимостями на различных уровнях. XSpider включает в себя функции сканера безопасности сайтов и позволяет проводить глубокий контроль защищенности WEB-серверов и WEB-приложений.

Функциональные возможности сетевого сканера XSpider:

* Полная идентификация сервисов на случайных портах

Дает возможность проверки на уязвимость серверов со сложной нестандартной конфигурацией, когда сервисы имеют произвольно выбранные порты

* Эвристический метод определения типов и имен серверов (HTTP, FTP, SMTP, POP3, DNS, SSH) вне зависимости от их ответа на стандартные запросы

Служит для определения настоящего имени сервера и корректной работы проверок в тех случаях, если конфигурация WWW-сервера скрывает его настоящее имя или заменяет его на другое

* Обработка RPC-сервисов (Windows и \*nix) с их полной идентификацией

Обеспечивает возможности определения RPC-сервисов и поиска уязвимостей в них, а также определения детальной конфигурации компьютера в целом

* Проверка слабости парольной защиты

Производится оптимизированный подбор паролей практически во всех сервисах, требующих аутентификации, помогая выявить слабые пароли

* Глубокий анализ контента WEB-сайтов

Анализ всех скриптов HTTP-серверов (в первую очередь, пользовательских) и поиск в них разнообразных уязвимостей: SQL инъекций, инъекций кода, запуска произвольных программ, получения файлов, межсайтовый скриптинг (XSS), HTTP ResponseSplitting.

* Анализатор структуры HTTP-серверов

Позволяет осуществлять поиск и анализ директорий доступных для просмотра и записи, давая возможность находить слабые места в конфигурации

* Проведение проверок на нестандартныеDoS-атаки

Существует возможность включения проверок "на отказ в обслуживании", основанных на опыте предыдущих атак и хакерских методах

* Специальные механизмы, уменьшающие вероятность ложных срабатываний

В различных видах проверок используются специально под них разработанные методы, уменьшающие вероятность ошибочного определения уязвимостей

* Ежедневное добавление новых уязвимостей и проверок

Оригинальная технология обновления программы не только позволяет пользователям каждый день иметь актуальную базу уязвимостей при минимальном трафике и временных затратах не прекращая при этом работы программы, но и обеспечивает регулярный update программных модулей по мере их совершенствования.

*3.ZecurionZserver (StorageSecurity)* является комплексом криптографических решений для защиты данных, которые хранятся на серверах, магнитных лентах, оптических дисках, в хранилищах и на внешних площадках. С помощью шифрования носителей ZecurionZserver (StorageSecurity) защищает данные в процессе использования, хранения и транспортировки.

*4.StaffCopEnterprise* – программа слежения за пользователями компьютеров в локальной сети и терминальных серверов. Продукт обеспечивает удаленный контроль за сотрудниками, анализ эффективности труда и защиту информации от утечек.

StaffCop осуществляет мониторинг запущенных программ, приложений и веб-сайтов на рабочих ПК. Выполняет перехват сообщений в ICQ, Skype, e-mail и других мессенджерах. Делает снимки экрана монитора, записывает нажатие клавиш и многое другое, входящее в понятие "контроль компьютера".

Мониторинг https-трафика, перехват сообщений по e-mail, skype, ICQ в социальных сетях и другие функции StaffCop позволят вам вовремя выявить попытки передачи корпоративных сведений сторонним лицам и получить доказательства для расследования инцидентов информационной безопасности. Блокировка USB-накопителей обеспечит защиту от копирования с рабочих компьютеров, данных, имеющих коммерческую ценность.

Оценочная стоимость предлагаемого комплекса программных продуктов представлена в табл. 12

Таблица 12

Оценочная стоимость предлагаемых продуктов

|  |  |
| --- | --- |
| Программный продукт | Стоимость, руб. |
| Касперскийдля Windows Servers Enterprise Edition | 5000 |
| Сканер уязвимостей XSpider | 85000 |
| ZecurionZserver (StorageSecurity) | 73000 |
| *StaffCopEnterprise* | 3500 |
| Итого | 166000 |

Таким образом, для защиты информации на предприятии необходимо провести комплекс мероприятий, который предполагает затраты на сумму 166 500 руб.

# 4.Разработка политики информационной безопасности.

Защищаемая информация:

Данные на бумажных носителях:

* договора (трудовые договора, договора на оказание услуг, договора сотрудничества и т.д.),
* акты (приема-передачи имущества (оборудования), о приемке выполненных работ и др.),
* деловые письма,
* протоколы совещаний,
* программы обучение персонала;

Электронные данные:

* бухгалтерская отчетность,
* планово-экономическая информация,
* информация об объемах выполненных работ;

Архивные документы:

* информация о сделках за прошлые периоды;
* документы о работе с поставщиками,
* отчетность и результаты работы автосервиса за предыдущие периоды;

Аналитическая отчетность, в этот актив входят следующие ресурсы:

* отчет по проведенным работам,
* отчет о персонале,
* отчет по оборудованию,
* отчет по затратам;

Персональные данные, для этого актива соответствуют следующие ресурсы:

* финансовые ведомости,
* сведения о клиентах,
* банковские реквизиты для осуществления расчетов с клиентами.

В идеале политика безопасности должна быть реалистичной и выполнимой, быть краткой и понятной, а также не приводить к существенному снижению общей производительности бизнес подразделений компании. Политика безопасности должна содержать основные цели и задачи организации режима информационной безопасности, четко содержать описание области действия, а также указывать на контактные лица и их обязанности.

Разработана избирательная политики безопасности.

Основные положения разработанной политики безопасности

**Введение**

Политика информационной безопасности Службы доставки зоотоваров «Гав’c» определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется в своей деятельности.

**Цели**

Основными целями политики ИБ являются защита информации организации и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Общее руководство обеспечением ИБ осуществляет директор автосервиса». Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет сотрудник отвечающий за функционирование автоматизированной системы и выполняющий функции администратора информационной безопасности.

Сотрудники учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

**Задачи**

Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба организации обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом, либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.[11]

Задачами настоящей политики являются:

* описание организации системы управления информационной безопасностью в Управлении;
* определение Политик информационной безопасности, а именно:
* определение порядка сопровождения ИС компании.

# Графическая часть

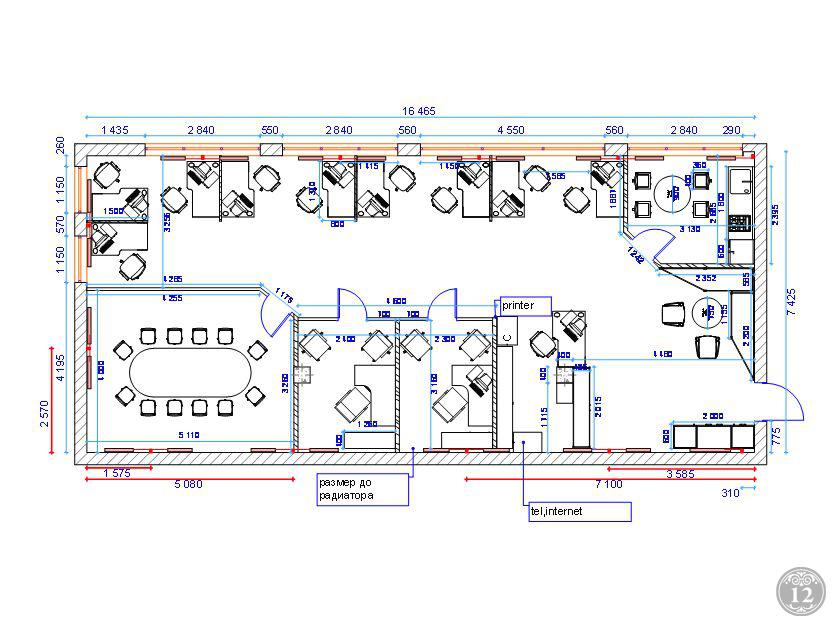


Рис.6 План помещения

|  |  |  |
| --- | --- | --- |
| *Наименование показателя* | *За 2014 год* | *За 2015 год* |
| Выручка | 5 722 | 8 202 |
| Валовая прибыль | 5 722 | 8 202 |
| Коммерческие расходы | - | - |
| Управленческие расходы | 2 976 | 4 582 |
| Прибыль от продаж | 2 746 | 3 620 |
| Чистая прибыль | 2 165 | 2 104 |

Табл. 1 Базовые экономические показатели Службы доставки зоотоваров «Гав’c»

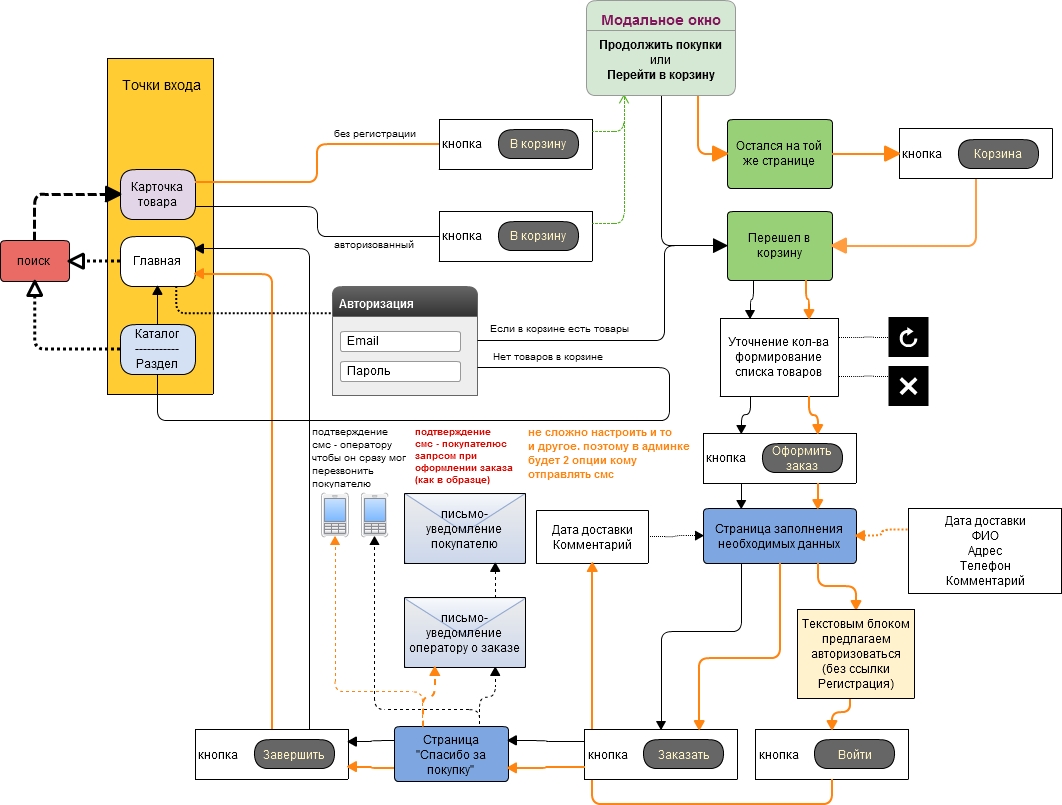
# Список используемой литературы

1. Бабаш. А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие/ А.В. Бабаш, Е.К.Баранова, Ю.Н. Мельников. –М.: КноРус, 2013. – 136с.
2. Гафнер. В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. –Рн/Д: Феникс, 2010. – 324с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2010.-384с.
4. Гулак М.Л., Рытов М.Ю. Основы компьютерной безопасности: Учеб. Пособие / Брян. гос. техн. ун-т.- Брянск: изд-во БГТУ, 2013.-215 с.
5. Обеспечение информационной безопасности машинострои-тельных предприятий: Учеб.для ВУЗа : в 2 ч.ч. 2 / Клейменов С.А., Мельников В.П., Схиртладзе А.Г., Борискин В.П. - Старый Оскол: ТНТ, 2011. 429 С
6. Коноплева И.А., Богданов И.А. Управление безопасностью и безопасность бизнеса: Учеб.пособие для вузов.- М.: ИНФРА-М, 2014. 446 с.
7. Зегжда, Д.П., Ивашко, А.М. Основы безопасности информационных систем. - М.: Интуит, 2010.
8. Стандарты информационной безопасности.
9. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. http://ru. wikipedia.org/wiki/
11. http://www.infosecurity.ru/

# 

# Приложения

**Приложение 1**



**Приложение 2**

