**Министерство сельского хозяйства РФ**

**Федеральное государственное бюджетное образовательное учреждение**

**высшего профессионального образования**

**«Пермская государственная сельскохозяйственная академия**

**имени академика Д. Н. Прянишникова»**

**Кафедра: *Информационных технологий и***

***автоматизированного проектирования***

# КУРСОВОЙ ПРОЕКТ

по дисциплине «Информационная безопасность»

на тему: «Разработка политики информационной безопасности ИП «Планета чудес»,

г. Краснокамск

**Проект выполнил**:

студент факультета Прикладной информатики

направления 080800

группы ПИб-41

Бабин Владимир Александрович

**Руководитель**:

доцент кафедры ИТАП,

к.э.н., доцент Глотина И.М.

## **Оценка** ………………………………

*…………………………………………*

*(дата защиты)*

*…………………………………………*

*(подпись преподавателя)*

### Пермь 2014

**Содержание**

[Введение 3](#_Toc386441146)

[1.Анализ системы информационной безопасности на предприятии 4](#_Toc386441147)

[1.1 Характеристика предприятия 4](#_Toc386441148)

[1.2 Анализ информационной безопасности на предприятии 5](#_Toc386441149)

[1.3 Анализ угроз информационной безопасности 6](#_Toc386441150)

[1.4 Предлагаемые мероприятия по созданию системы защиты информации 8](#_Toc386441151)

[2.Создание системы информационной безопасности 9](#_Toc386441152)

[3.Эффективность формирования системы ИБ 13](#_Toc386441153)

[Заключение 15](#_Toc386441154)

[Список использованных источников 16](#_Toc386441155)

[Приложение 17](#_Toc386441156)

[Политика безопасности ИП «Планета чудес», г. Краснокамск 17](#_Toc386441157)

[1.Общие положения и цели 17](#_Toc386441158)

[2.Управление информационной безопасностью 17](#_Toc386441159)

[3.Ответственность 18](#_Toc386441160)

[4.Заключительные положения 18](#_Toc386441161)

# Введение

Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации.

Проблема обеспечения информационной безопасности стоит перед каждым предприятием вне зависимости от его масштабов, числа работников или формы собственности. Ведь даже если, к примеру, самому предприятию не так уж важны личные данные своих клиентов, то согласно федеральному закону 152-ФЗ «О персональных данных» лица, виновные в нарушении требований этого закона несут ответственность вплоть до уголовной. Однако в большинстве случаев информационная безопасность обеспечивается не из страха перед законом, а сама является важной частью менеджмента организации, обеспечивающая эффективность бизнес-процессов и решающая не только тактические, но и стратегические задачи. Потеря этой информации может привести к самым плачевным последствиям.

Задачи курсового проекта:

1. Проанализировать структуру организации
2. Проанализировать информационные ресурсы организации
3. Проанализировать систему информационной безопасности;
4. Выявить недостатки существующей системы информационной безопасности и предложить мероприятия по их устранению;
5. Создать политику безопасности организации;

Цель: обеспечение информационной безопасности предприятия.

1. **Анализ системы информационной безопасности на предприятии**

## **1.1 Характеристика предприятия**

Наименование предприятия – ИП Зайчикова Ольга Александровна

Юридический адрес – 617060, Пермский край, г. Краснокамск, ул. Чапаева, д. 25, кв. 15

Адрес офиса – 617060, Пермский край, г. Краснокамск, ул. Большевистская, 12

Телефон – 8-964-186-12-83, (34273) 9-88-18

E-mail – planetachudes@mail.ru

ОГРН – 310591615400021

ИНН – 591602004478

Основной вид деятельности – продажа туристического продукта (комплекса услуг, работ, товаров, необходимых для удовлетворения потребностей туриста в период его туристского путешествия).

По организационно-правовой форме предприятие является индивидуальным предпринимателем. Индивидуальные предприниматели — физические лица, зарегистрированные в установленном законом порядке и осуществляющие предпринимательскую деятельность без образования юридического лица.

На предприятии присутствует ноутбук Samsung R519 с процессором Intel Pentium Dual-Core T3400 2.16 ГГц, интегрированной видеокартой, 4Гб оперативной памяти и 160 Гб HDD. На нем установлен и постоянно используется для работы следующий перечень программного обеспечения:

- OS Windows Vista (предустановленная на момент покупки);

- КалендарьWindows;

- ПочтаWindows;

- AVG AntiVirus FREE Edition;

- Microsoft Office;

- Google Chrome;

- Adobe Reader;

- Skype;

- ICQ Messenger;

- 2ГИС;

- Налогоплательщик;

- Консультант+;

- Десктопные системы бронирования туроператоров: Мастер Агент, Мастер-Тур, КСБ Алеан.

Для планирования рабочего времени и напоминаний используется встроенный календарь Windows. Подавляющая часть работы осуществляется через браузер и почтовый клиент. Для переговоров с туроператорами часто используется Skype и ICQ. Для подготовки документов наиболее часто используются MS Word. Десктопные системы бронирования почти не используются, заменяясь веб-интерфейсом сайтов туроператоров.

## **1.2 Анализ информационной безопасности на предприятии**

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надёжность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в неё изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи.

Разумеется, во всех цивилизованных странах на страже безопасности граждан стоят законы, но в сфере вычислительной техники правоприменительная практика пока развита недостаточно, а законотворческий процесс не успевает за развитием технологий, поэтому надёжность работы компьютерных систем во многом опирается на меры самозащиты.

Существуют три метода реализации самозащиты:

- программные методы защиты;

- аппаратные методы защиты;

- организационные методы защиты.

Программные методы защиты на предприятии присутствуют в виде антивируса AVG AntiVirus бесплатной версии.

AVG Antivirus — антивирусная система, имеющая сканер файлов, сканер электронной почты и поддерживающая возможность автоматического наблюдения. Одним из серьезных минусов данного антивируса является отсутствие брандмауэра. Он так же не установлен и отдельно, что является серьезным риском для безопасности при постоянной работе в сети Интернет. Единственная надежда сейчас только на встроенный брандмауэр Windows Vista.

Ноутбук часто подвергается переноске (в том числе за пределы офиса), где с ним может случиться всё что угодно, от повреждения HDD и вплоть до кражи. При этом резервная копия данных (backup) на других носителях отсутствует.

С целью недопущения доступа к информации посторонних лиц используется стандартная авторизация Windows для входа в систему. Этого, разумеется, недостаточно для обеспечения безопасности данных при попадании ноутбука в чужие руки.

Политика безопасности как такая отсутствует.

Информационные ресурсы на предприятии делятся на две группы:

1. Конфиденциальная информация (личные данные о сотрудниках фирмы, личные данные клиентов, бухгалтерская отчетность, финансовое положение)
2. Открытая информация (сведения о предприятии, сведения о предложениях предприятия)

**1.3 Анализ угроз информационной безопасности**

В общем случае под угрозой принято понимать потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. В свою очередь, угроза информационной безопасности автоматизированной системы - это возможность реализации воздействия на информацию, приводящего к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность воздействия на компоненты автоматизированной системы, приводящего к их утрате, уничтожению или сбою функционирования.

В зависимости от источника угрозы принято выделять:

* угрозы, источником которых является природная среда. Примеры таких угроз - пожары, наводнения и другие стихийные бедствия.
* угрозы, источником которых является человек. Примером такой угрозы может служить внедрение агентов в ряды персонала автоматизированных систем со стороны конкурирующей организации.
* угрозы, источником которых являются санкционированные программно-аппаратные средства. Пример такой угрозы: некомпетентное использование системных утилит.
* угрозы, источником которых являются несанкционированные программно-аппаратные средства. К таким угрозам можно отнести, например, внедрение в систему кейлоггеров,  Кейлоггер (анг. Keylogger key(stroke) - нажатие на клавишу и англ. logger - регистрирующее устройство) - это программный продукт (модуль) или аппаратное устройство, регистрирующее каждое нажатие клавиши на клавиатуре компьютера.

По положению источника угрозы выделяют:

* угрозы, источник которых расположен вне контролируемой зоны. Примеры таких угроз - перехват побочных электромагнитных излучений (ПЭМИН) или перехват данных, передаваемых по каналам связи; дистанционная фото и видеосъёмка; перехват акустической информации с использованием направленных микрофонов;
* угрозы, источник которых расположен в пределах контролируемой зоны. Примерами подобных угроз могут служить применение подслушивающих устройств или хищение носителей, содержащих конфиденциальную информацию;

На конкретном рассматриваемом предприятии можно выделить следующие недостатки в безопасности:

* отсутствуют средства резервного копирования;
* отсутствует шифрование данных;
* отсутствует firewall;
* велика вероятность физической кражи носителей информации;

## **1.4 Предлагаемые мероприятия по созданию системы защиты информации**

Разработать политику информационной безопасности. Запретить выносить оборудование за пределы офиса. Обновить программное обеспечение, настроить резервное копирование.

1. **Создание системы информационной безопасности**

Приступая к разработке системы информационной безопасности, необходимо отметить, что прочность цепи равна прочности слабейшего звена. В данном случае самым слабым звеном в цепи, как правило, является не протокол, программа или машина, а человек (администратор, пользователь, а то и руководитель). А также что нет никакого смысла сочинять и подписывать какие-то инструкции по безопасности, если они не будут читаться и неукоснительно исполняться всеми сотрудниками организации.

Если с этим проблем нет, то сама политика информационной безопасности должна быть гибкой и учитывать специфику предметной области конкретного предприятия. Скорее всего не имеет смысла. тратить большие ресурсы на обеспечение защиты от всех видов угроз, тем более для защиты не особо критичных данных. Конечно, все данные, необходимые для работы, должны быть защищены от случайной утраты, от несанкционированного доступа, но степень этой защиты и средства для её обеспечения должны всегда определяться здравым смыслом. Расходы на защиту не должны превышать стоимости защищаемой информации.

Необходимо также жестко ограничить права доступа сотрудникам только теми возможностями, которые требует их должность.

В политике должны быть закреплены только основные положения, ведь предприятие — динамичная система, которая находится в процессе непрерывного развития. Конкретные должностные инструкции для сотрудников, различные документации необходимо разрабатывать отдельно. Их существование обеспечивает должный уровень прозрачности как для внутреннего использования на предприятии, так и даст возможность привлекать внешних экспертов для оценки качества системы информационной безопасности. А без этого невозможно понять, что инфраструктура предприятия сделана как надо и обходится по адекватной цене.

Что остается самым распространенным методом аутидентификации на сегодняшний день? Конечно же, парольная аутентификация. Это ввод чего-либо, что известно только пользователю, например, пароля или ответа на секретный вопрос. Теоретически, это самый простой и безопасный метод проверки подлинности, так как он обладает достаточной криптостойкостью, его просто и дешево реализовать, а всё что нужно от пользователя, так это запомнить 8-12-ти символьную комбинацию из букв, цифр и различных знаков. Однако, на практике всё совершенно иначе.

Во-первых, пользователи, как правило, задают слабые пароли, что связано с самой физиологией человека, точнее его мозга. Наше мышление ассоциативно и напрямую связано с речью, мы мыслим образами, каждый из которых имеет название, поэтому в качестве пароля мы выбираем название одного из них. Таким образом большинство паролей задаваемых пользователями мы можем найти в обычном словаре, а потому они легко подбираются методом перебора по словарю. О слабой криптостойкости выбираемых пользователями паролей написано множество статей. Одна из самых старых датируется 1990 годом. В ней Дэниель Клейн описывает, то как он вооружившись словарём из 62 727 слов смог за пару недель подобрать пароли к 3 340 учётным записям, что составило 24,2% от общего количества [2]. Стоит при этом отметить два фактора:

1. Люди не стали задавать более сложные пароли с тех пор.

2. Согласно «закону Мура» вычислительные мощности компьютеров с тех пор выросли более чем в 16 тысяч раз.

Конечно, с тех пор проведено множество исследований и на их основе предложено немало систем построения сложных паролей на основе мнемонических фраз. Но в процентном отношении, мало кто ими пользуется.

К тому же, несмотря ни на какие чудо-системы, с ростом сложности пароля он всё труднее для запоминания. Исследование SafeNet от 2004 года обнаружило, что 47 % респондентов забывали свои пароли в течение года. А с ростом количества учётных записей от различных компьютерных систем, которых с каждым годом становится всё больше, ситуацию ещё более усугубляется. Способность помнить пароли была изучена в лаборатории Ву в 2007 году. После первой недели 12.5 % участников забыли их шестисимвольные буквенно-цифровые пароли. Из участников, которые должны были помнить пароли о пяти учетных записей, 25 % забыли по крайней мере один.

Кроме того, с увеличением сложности паролей увеличивается и количество ошибок при его вводе. Например, Бростофф и Сэйсс заметили, что разрешение на ввод до десяти неправильных паролей подряд уменьшает количество запросов на их сброс. Собственно, после этого исследования многие компании скорректировали свои парольные политики.

Но даже это не самое страшное. Исследование, проведённое Джоном Лейдоном в 2003 году, выявило пугающую склонность офисных работников сообщать свои пароли незнакомцам за символическую плату. В исследовании приняло участие 152 человека. Им была задана серия вопросов, один из которых просил указать пароль пользователя, и 75% опрошенных немедленно его назвали. Они раскрыли свой пароль в обмен на безделушку стоимостью меньше одного фунта стерлингов.

Следующий по распространённости механизм аутентификации обычно используют если пароль всё-таки утерян. Тогда пользователя просят ответить на так называемый «секретный вопрос», ответ на который он указал при регистрации учётной записи. Именно такая система используется у 4 ведущих почтовых провайдеров AOL, Google (Gmail), Microsoft (Hotmail), и Yahoo!.

Однако, криптостойкость подобных «вопрос и ответов», выбираемых пользователями, ещё меньше, чем у выбираемых ими паролей. В 2009 году на конференции IEEE Security and Privacy был опубликован доклад о исследовании, в котором приняло участие 130 человек. Результаты показали, что чуть менее трети испытуемых – 28 процентов – смогли «угадать» ответ на секретный пароль, в случае если близко знали своего оппонента. Если же оппонент был полностью незнаком, то ответ на вопрос угадали 17 процентов испытуемых. Впрочем, конечный результат во многом зависит от сложности поставленного вопроса. Например, вопрос о любимой команде пользователя или его любимом городе не станет большой проблемой в 30 и 57 процентах случаев соответственно. Но даже на вопросы личного характера – город рождения, или кличка домашнего питомца – взломщик дает правильный ответ в 45 и 40 процентов случаев соответственно. Кроме того, по прошествии от 3-х до 6-ти месяце 49 участников попросили вспомнить свои ответы, 16% их забыли. Ранее в 2008 году Ариель Рабкин провёл похожее исследование, гласящее что многие из «секретных вопросов» были или не применимыми к более чем 15 % широкой публики, незапоминающимися, неоднозначными, легко отгадываемыми даже при отсутствии информации о жертве, либо легко отгадываемыми с минимальным знанием жертвы. Аналогичные работы проходили и ранее в 1996-м и в 1990-м годах. Они тоже исследовали способность запоминать и угадывать ответы на «секретные вопросы». И показали похожие результаты, а именно: супруги и близкие друзья могли угадать 33%-39% ответов, а 20%-22% забыли свои ответы в течение 3-х месяцев.

Интересная работы была опубликована в позапрошлом году. Её целью было выяснить криптостойкость ответов на «секретные вопросы» сами по себе. С этой целью авторы собрали огромную базу данных (порядка 269 млн.) имён, фамилий, кличек домашних животных, дат и мест рождения пользователей. При анализе этих данных выяснилось, что они подчиняются распределению Ципфа, частным случаем которого является «закон Парето», т.е. на 20% имён и дат приходилось 80% пользователей. В результате, оказалось, что криптостойкость ответов на данные «секретные вопросы» соответствует криптостойкости ключа шифрования длинной от 8 до 23 бит, в зависимости от распространённости конкретного имени или фамилии.

Всё это свидетельствует о том, что сложность пароля и методы его хранения необходимо закрепить в политике безопасности.

1. **Эффективность формирования системы информационной безопасности**

Систему информационной безопасности необходимо постоянно совершенствовать. Мир вокруг меняется: постоянно появляются новые виды угроз и совершенствуются существующие. Но и по другую сторону баррикад жизнь не стоит на месте. Для обеспечения информационной безопасности нужно постоянно быть в курсе этого противостояния и стараться использовать самые новые методы защиты и стараться предусмотреть все возможные угрозы и возможные действия злоумышленников. При этом разработчик политики и системы в целом должен помнить о двух важных моментах:

* Целевая аудитория политики ИБ — конечные пользователи и топ-менеджмент компании, которые не понимают сложных технических выражений, однако должны быть ознакомлены с положениями политики.
* Не нужно пытаться включить в этот документ все, что можно. Здесь должны быть только цели ИБ, методы их достижения и ответственность. Никаких технических подробностей, если они требуют специфических знаний. Это все — материалы для инструкций и регламентов.

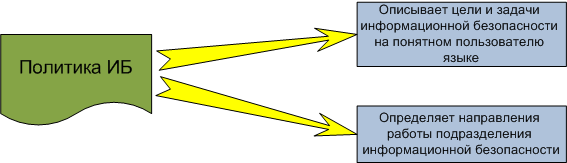


Рисунок 1 – политика ИБ

А также что необходимо обеспечить:

* лаконичность — большой объем документа отпугнет любого пользователя и этот документ никогда не прочитают;
* доступность простому обывателю — конечный пользователь должен понимать, ЧТО написано в политике (он никогда не прочитает и не запомнит слова и словосочетания «журналирование», «модель нарушителя», «инцидент информационной безопасности», «информационная инфраструктура», «техногенный», «антропогенный», «риск-фактор» и т.п.)

Политика ИБ должна быть документом первого уровня, ее должны расширять и дополнять другие документы (положения и инструкции), которые уже будут описывать что-то конкретное.

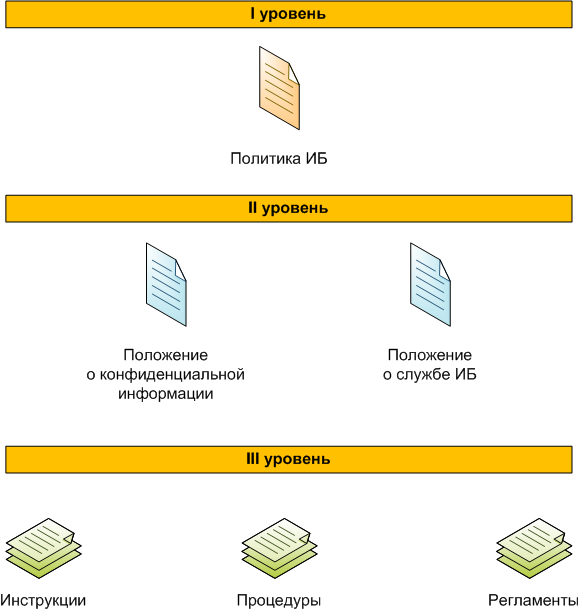


Рисунок 2 – структура документов, описывающих информационную безопасность предприятия

# Заключение

В процессе выполнения курсового проекта был проведен анализ средств информационной безопасности ИП «Планета чудес», информационных ресурсов предприятия, проанализированы угрозы информационной безопасности, выявлены ее недостатки и предложены пути их устранения. Разработана политика информационной безопасности.

# Список использованных источников

1. Э.Р. Газизова, Л.Т. Веденьев, А. Афанасьев, А.В. Воронцов. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов, 2009 г.
2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 23.07.2013) "О персональных данных"
3. Социальный хакинг в быту (защищаемся от глупостей) - Режим доступа: <http://habrahabr.ru/post/79449/>, свободный. - Загл. с тит. экрана.
4. Классификация механизмов аутентификации пользователей и их обзор) - Режим доступа: <http://habrahabr.ru/post/177551/>, свободный. - Загл. с тит. экрана.
5. Политика информационной безопасности — опыт разработки и рекомендации - Режим доступа: <http://habrahabr.ru/post/174489/>, свободный. - Загл. с тит. экрана.

# Приложение Б

Утверждена

решением руководителя

ИП «Планета чудес»

от 28 апреля 2014 года

Протокол №1

## **Политика безопасности**

## **ИП «Планета чудес», г. Краснокамск**

* + - 1. **Общие положения и цели**
  1. ИП «Планета чудес» является предприятием, осуществляющим деятельность в сфере туризма. Осуществление указанной деятельности связано с управлением информацией, являющейся важным активом ИП «Планета чудес», и зависит от обеспечения информационной безопасности, под которой понимается обеспечение конфиденциальности, целостности и доступности информационных активов.
  2. Политика информационной безопасности ИП «Планета чудес» устанавливает цели, задачи и подходы в области информационной безопасности, которыми ИП «Планета чудес» руководствуется в своей деятельности.
  3. Политика направлена на достижение следующих целей: обеспечение непрерывности основных бизнес-процессов ИП «Планета чудес»: минимизацию возможных потерь и ущерба от нарушений в области информационной безопасности.
     + 1. **Управление информационной безопасностью**

2.1 Необходимо обеспечить резервное копирование критичных для работы данных.

2.3 Выносить оборудование за пределы офиса запрещается.

2.2 Любой рабочий пароль должен:

* + - содержать не менее 10 символов;
    - содержать символы, набранные в разных регистрах;
    - помимо латинских букв, содержать также цифры, знаки препинания и/или специальные символы;
    - не являться словом из словаря, сленга, диалекта, жаргона;
    - не являться персональной информацией (имена, адреса, дата рождения, телефон и т.п.)

2.3 Производить изменение паролей в критичных для работы учетных записях необходимо не реже чем раз в месяц.

**3. Ответственность**

3.1 Руководство ИП «Планета чудес» осуществляет общее управление информационной безопасностью ИП «Планета чудес» и обеспечивает необходимые условия для:

* + - * реализации мероприятий по оценке рисков информационной безопасности и защиты информации;
      * поддержания, мониторинга, анализа и непрерывного улучшения системы управления информационной безопасностью;
      * регулярного обучения работников ИП «Планета чудес» в сфере информационной безопасности.

4**. Заключительные положения**

4.1 Руководство ИП «Планета чудес» заявляет своё одобрение настоящей Политики, которая объявлена, распространена, внедрена и поддерживается на всех уровнях ИП «Планета чудес».

4.2 Политика информационной безопасности ИП «Планета чудес» является общедоступным документом, который может предоставляться всем заинтересованным сторонам и размещается на официальном веб-сайте ИП «Планета чудес».