МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский Государственный Технологический Университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

Лабораторная работа №3

«Разработка политики информационной безопасности авиакомпании»

Выполнил:

студент 3 курса, 4 группы

Чернявский А. Л.

Проверила:

Копыток Д. В.

Минск 2020

**ОГЛАВЛЕНИЕ**

[**1.** **ВВЕДЕНИЕ.** 3](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163564)

[**2.** **ПОСТАНОВКА ЗАДАЧИ** 4](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163565)

[**3.** **СПЕЦИФИКА РУКОВОДСТВА АВИАКОМПАНИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** 5](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163566)

[**3.1.** **ОХРАНЯЕМЫЕ СВЕДЕНИЯ В ОРГАНИЗАЦИИ** 5](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163567)

[**3.2.** **ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ ОХРАНЯЕМЫХ СВЕДЕНИЙ И ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ** 5](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163568)

[**3.3.** **ОЦЕНКА ВОЗМОЖНОСТЕЙ ТЕХНИЧЕСКИХ РАЗВЕДОК И ДРУГИХ ИСТОЧНИКОВ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ** 5](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163569)

[**3.4.** **ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ ПО ЗАЩИТЕ ИНФОРМАЦИИ** 6](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163570)

[**3.5.** **ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ И КОНТРОЛЮ** 6](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163571)

[**3.6.** **КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ** 6](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163572)

[**3.7.** **ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ ПРЕДПРИЯТИЯМИ** 7](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163573)

[**4.** **ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВИАКОМПАНИИ** 8](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163574)

[**5.** **МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ** 9](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163575)

[**6.** **ВЫВОД** 11](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163576)

[**7.** **СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ** 12](file:///C:\Users\Alexey%20Chernyavsky\Downloads\Univer\6SEMESTR\KMZI\labs\lab1\электронный%20конспект.docx#_Toc477163577)

# **ВВЕДЕНИЕ.**

Политика информационной безопасности – это высокоуровневый документ, который включает в себя принципы и правила, определяющие и ограничивающие определенные виды деятельности объектов и участников системы информационной безопасности, направленные на защиту информационных ресурсов организации.

Как известно, стратегическое планирование позволяет определить основные направления деятельности организации, связав воедино маркетинг, производство и финансы. Долгосрочный стратегический план позволяет компании выстроить все свои бизнес-процессы с учетом микро и макросреды для достижения наилучших финансовых показателей и темпов экономического роста. Важной составляющей в стратегическом планировании является учет требований политики информационной безопасности, которые должны быть краеугольным камнем при определении среднесрочных и долгосрочных целей и задач организации. С ростом компании и пересмотром планов политика также должна пересматриваться. Низкоуровневые документы информационной безопасности необходимо пересматривать в соответствии с реализацией краткосрочных планов.

Политика информационной безопасности неразрывно связана с развитием компании, ее стратегическим планированием, она определяет общие принципы и порядок обеспечения информационной безопасности на предприятии. Политика информационной безопасности тесно интегрируется в работу предприятия на всем этапе его существования. Все решения, предпринимаемые на предприятии, должны учитывать её требования.

Основные этапы разработки политики информационной безопасности следующие:

* исследование текущего состояния информационной среды и информационной безопасности организации;
* анализ полученных сведений по результатам исследования;
* формирование плана работ по разработке политики информационной безопасности;
* разработка политики информационной безопасности организации;

# **ПОСТАНОВКА ЗАДАЧИ**

В данной работе требуется изучить информационную систему авиакомпани. Для этого необходимо выделить участки с наиболее важной информацией, уделить внимание изучению различных путей нанесения вреда: уничтожение информации, физическое повреждение носителей информации, программное повреждение информации (вирусы). На основании полученных данных разработать план по выявлению угроз и их устранению.

Конечный документ должен удовлетворять следующим требованиям:

* лаконичность – большой объем документа отпугнет любого пользователя, ваш документ никто никогда не прочитает.
* доступность простому обывателю – конечный пользователь должен понимать, что написано в политике о защите информации.

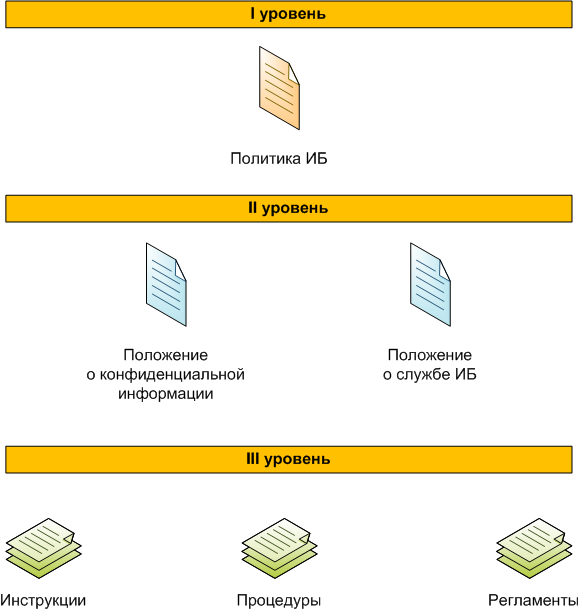


Рис.1 Структура написания политики информационной безопасности.

На самом деле все очень просто: политика ИБ должна быть документом первого уровня, ее должны расширять и дополнять другие документы (положения и инструкции), которые уже будут описывать что-то конкретное.

# **СПЕЦИФИКА РУКОВОДСТВА АВИАКОМПАНИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Руководство должно состоять из следующих разделов:

1. Охраняемые сведения в организации;
2. Демаскирующие признаки охраняемых сведений и технические каналы утечки информации;
3. Оценка возможностей технических разведок и других источников угроз безопасности информации;
4. Организационные и технические мероприятия по защите информации;
5. Обязанности и права должностных лиц по защите информации;
6. Планирование работ по защите информации и контролю;
7. Контроль состояния защиты информации;
8. Взаимодействие с другими предприятиями (учреждениями, организациями), КГБ.

Расскажем немного о каждом из разделов.

## **ОХРАНЯЕМЫЕ СВЕДЕНИЯ В ОРГАНИЗАЦИИ**

В этом разделе указывается конкретная цель, которая должна быть достигнута в результате проведения мероприятий по защите информации (охраняемых сведений) в компании, замысел достижения этой цели и приводится перечень охраняемых сведений (без указания конкретных числовых параметров).

## **ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ ОХРАНЯЕМЫХ СВЕДЕНИЙ И ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ**

В этом разделе указываются демаскирующие признаки, которые раскрывают охраняемые сведения в авиакомпании, в том числе демаскирующие признаки, возникающие в связи с использованием средств обеспечения ее деятельности. Приводятся возможные технические каналы утечки охраняемых сведений, включая каналы утечки информации в технических средствах ее обработки.

## **ОЦЕНКА ВОЗМОЖНОСТЕЙ ТЕХНИЧЕСКИХ РАЗВЕДОК И ДРУГИХ ИСТОЧНИКОВ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

В этом разделе приводится перечень видов и средств технической разведки, источников угроз несанкционированного доступа к информации, которые опасны для данной организации, в том числе со стороны преступных группировок и результаты оценки их возможностей: по обнаружению демаскирующих признаков, раскрывающих охраняемые сведения; по перехвату информации, циркулирующей в технических средствах ее обработки; по перехвату речевой информации из помещений; по получению, разрушению (уничтожению), искажению или блокированию информации в результате несанкционированного доступа к ней.

При оценке используется частная модель угроз для организации, методики оценки возможностей иностранной технической разведки и другие документы по этому вопросу.

В разделе "Организационные и технические мероприятия по защите информации" приводятся:

* организационные и технические мероприятия, обеспечивающие устранение или ослабление (искажение) демаскирующих признаков и закрытие возможных технических каналов утечки охраняемых сведений в организации;
* мероприятия по защите информации об иной создаваемой (применяемой) продукции и технологиях;
* мероприятия по защите информации при постоянном контролируемом и неконтролируемом нахождении иностранных граждан как на территории организации, так и в непосредственной близости от нее;
* мероприятия по защите информации в системах и средствах информатизации и связи.

## **ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ ПО ЗАЩИТЕ ИНФОРМАЦИИ**

В этом разделе определяются должностные лица подразделений авиакомпании, ответственные за разработку, обеспечение и выполнение мероприятий по защите информации, их функциональные обязанности и права, приводится структурная схема взаимодействия подразделений по защите информации с соответствующими основными подразделениями организации.

## **ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ И КОНТРОЛЮ**

В этом разделе указываются руководящие документы для планирования работ по защите информации, требования к содержанию планов, приводится порядок разработки, согласования, утверждения и оформления планов, устанавливается порядок отчетности и контроля за выполнением планов.

## **КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ**

В разделе "Контроль состояния защиты информации" указываются задачи контроля, перечень органов и подразделений, имеющих право проверки состояния защиты информации в организации, привлекаемые силы и средства контроля, порядок привлечения (при необходимости) к этой работе специалистов основных подразделений организации, устанавливаются периодичность и виды контроля, порядок оформления результатов контроля, определяются действия должностных лиц по устранению нарушений норм и требований по защите информации и порядок разработки мероприятий по устранению указанных нарушений.

## **ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ ПРЕДПРИЯТИЯМИ**

В этом разделе указываются порядок взаимодействия в области защиты информации с предприятиями (учреждениями, организациями) при выполнении совместных работ, применяемые совместные организационные и технические мероприятия по защите информации, ответственность, права и обязанности взаимодействующих сторон, а также приводится структурная схема взаимодействия.

# **ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВИАКОМПАНИИ**

Пассажир при бронировании сообщает авиакомпании или агенту по продаже перевозок необходимую информацию о маршруте перевозки, дате и времени вылета, необходимом количестве бронируемых мест, классе обслуживания на борту воздушного судна, имеющемся гражданстве, а также информацию о своих персональных данных.  В случае отказа пассажира от предоставления информации, необходимой для бронирования, бронирование не производится. Пассажир при бронировании может сообщить номер телефона или иной способ контакта для его информирования.

Информация личного характера, полученная в формате бумажных регистрационных форм или через сайт компании, используется, среди прочего, для целей регистрирования пользователей, отслеживания политики и статистики, а также в целях, разрешенных пассажиром. Кроме того, авиакомпания использует информацию личного характера для поддержания связи с клиентами иными способами. Информация также используется для того, чтобы проинформировать о внесении существенных изменений в настоящую Политику информационной безопасности. Время от времени пользователям сайта компании предлагается предоставлять информацию в формате опросов или анкет.

Авиакомпания нанимает другие компании, которые предоставляют услуги, такие как обработка и доставка информации, размещение информации, доставка содержания и услуг на сайт компании, выполнение статистического анализа. Чтобы эти компании могли предоставлять эти услуги, авиакомпания сообщает им информацию личного характера, однако им будет разрешено получать только ту информацию личного характера, которая необходима им для предоставления услуг. Они обязаны соблюдать конфиденциальность этой информации, и им запрещено использовать ее в иных целях.

Авиакомпания может использовать или раскрывать личные данные потребителя и по иным причинам, в том числе, если мы считаем, что это необходимо в целях выполнения требований закона или решений суда, для защиты прав или собственности компании, защиты личной безопасности пользователей нашего сайта и других соглашений, в целях расследования или принятия мер в отношении незаконной или предполагаемой незаконной деятельности, в связи с корпоративными сделками, такими как разукрупнение, слияние, продажа активов или в маловероятном случае банкротства, или в иных целях в соответствии с вашим согласием. авиакомпания может раскрывать содержание сообщений или писем, однако не будет размещена или опубликована информацию личного характера, а также, за исключением случаев, предусмотренных в настоящей Политике конфиденциальности, такая информация не будет предоставляться оказывающим услуги третьим сторонам без вашего согласия. Информация не будет продана, предоставлена на правах аренды или лизинга, наши списки пользователей с адресами электронной почты третьим сторонам.

# **МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ**

Информационная безопасность в сфере гражданской авиации достигается своевременным принятием ряда мер и определенных средств защиты в авиакомпаниях, аэропортах и в компаниях-контрагентов.

1. **Организационные меры.** В первую очередь, защита информации должна начинаться с человека, сотрудника который возьмёт на себя обязанность по обеспечению информационной безопасности в компании. Если компания очень большая, то одним сотрудником не обойтись, и лучше создать отдел хотя бы из 3 человек, один руководитель и два инженера. В любом случае сотрудник или руководитель отдела должен хорошо разбираться в вопросах защиты информации, уровень компетенции сотрудника обязательно отразится на финансовых затратах на защиту информации. Когда сотрудника нашли - он после изучения информационных процессов в компании должен разработать соответствующие организационно-распорядительные документы, подписываются которые главным лицом в компании.
2. **Физические меры** - ограничение физического доступа к защищаемой информации.
3. **Технические меры** - разнообразные средства защиты от НСД, защита информации от утечки по техническим каналам связи, криптографические средства защиты информации, системы защиты от DDOS-атак

Существуют средства защиты информации:

* средства защиты от внешних угроз – антивирусы (Kaspersky AntiVirus for Mail servers, Dr.Web Enterprise Suite и т. д.) средства защиты от DDoS-атак, межсетевые экраны и т. п.;
* средства защиты от внутренних угроз - DLP-системы (InfoWatch, [McAfee DLP](javascript:void(0);)), защита баз данных, системы разделения доступа к информационным ресурсам.
* средства резервирования. Аппаратные и программные средства создания backup (Veeam® Endpoint Backup).

Также существуют не только средства, но и методы (принципы защиты информации):

Препятствование – метод физической защиты информационных систем (ИС), благодаря которому злоумышленники не имеют шанса попасть на охраняемую территорию или к защищаемой информации (к оборудованию, дискам и так далее).

Управление доступом – при этом методе защиты информации регулируется и контролируется эксплуатирование ресурсов компьютерной ИС (компонентов БД, программного обеспечения и аппаратуры). Управление доступом несет множество защитных функций:

* распознавание пользователей, работников и ресурсов системы (всем объектам присваивается персональный идентификационный код);
* аутентификация (установление подлинности) объекта или субъекта согласно представляемого им идентификационному коду;
* инспекция уровня доступа, то есть проверяется согласованность идентификационного кода, даты и времени суток, уровень и вид запрашиваемых ресурсов и операций принятым правилам;
* предоставление доступа и создание условий работы в пределах существующего регламента;
* фиксация (внесение в протокол) запросов к защищаемым ресурсам;

Маскировка – технология охраны данных, ограждающая доступ к ней c помощью криптографии (информация видоизменяется так, что третьи лица без понимания принципа шифровки не имеют возможности ее воспринимать). Этот способ является единственной надежной гарантией защиты данных при передаче их по каналам связи большой протяженности.

# **ВЫВОД**

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.

# **СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ**

1 Как обеспечить информационную безопасность в авиакомпаниях [Электронный ресурс] / Все о туризме. Туристическая библиотека. 2017 г. URL: http://tourlib.net/statti\_tourism/suhanov.htm (дата обращения: 28.02.2020).

2. Политика информационной безопасности [Электронный ресурс] / Официальный сайт белорусских авиалиний «BELAVIA». 2017 г. URL: https://belavia.by/policy (дата обращения: 28.02.2020).

3. Меры защиты информации [Электронный ресурс] / Методы защиты информации кратко. 2017 г. URL: http://interesting-information.ru/2015/07/metody-zashhity-informacii-kratko (дата обращения: 28.02.2020).

4. Основное содержание руководства по защите информации [Электронный ресурс] / Электронный фонд правовой и нормативно-технической документации. 2017 г. URL: http://docs.cntd.ru/document/902015340 (дата обращения: 28.02.2020).

5. Политика информационной безопасности [Электронный ресурс] / Политика информационной безопасности – опыт разработки и рекомендации. 2017 г. URL: https://habrahabr.ru/post/174489/ (дата обращения: 28.02.2020).