БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №1**

**«**Разработка политики безопасности для туристической компании»

Выполнила:

студентка 3 курса 4 группы

Невар Юлия Валерьевна

Проверила:

Блинова Е.А.

Минск 2021

**Содержание**

[1. Обоснование актуальности, цели и задачи разработки ПИБ в организации 3](#_Toc63839695)

[2. Объекты защиты 4](#_Toc63839696)

[3. Основные угрозы и их источники 6](#_Toc63839697)

[4. Оценка угроз, рисков, и уязвимостей 7](#_Toc63839698)

[5. Меры, методы и средства обеспечения требуемого уровня защищённости 10](#_Toc63839699)

[Выводы и предложения 11](#_Toc63839700)

# **1. Обоснование актуальности, цели и задачи разработки ПИБ в организации**

Политика компании в области информационной предусматривает принятие необходимых мер в целях защиты ресурсов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в туристической компании.

Информация существует в различных формах: на бумажном носителе, в электронном виде при хранении на носителе, передается по почте или с использованием электронных устройств, передаваться устно в процессе общения. Информация должна быть защищена независимо от ее формы и способа ее распространения, передачи и хранения.

Информационная безопасность — это защита информации от различных угроз, призванная обеспечить непрерывность бизнес-процессов, минимизировать риски и обеспечить возможности служебной деятельности.

Главные цели компании не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник компании. На лиц, работающих в туристической компании по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей политики распространяются в случае, если это обусловлено в таком договоре.

Целью политики является создание условий, позволяющих предотвратить или минимизировать ущерб, который может быть нанесен в результате несанкционированного доступа, хищения служебной информации или нанесения ущерба техническим средствам обработки, хранения и передачи защищаемой информации.

Под защитой информационных ресурсов следует понимать:

* сохранение конфиденциальности информационных ресурсов;
* обеспечение непрерывности доступа к информационным ресурсам компании в сферах его деятельности;
* защита целостности служебной информации с целью поддержания возможности компании по оказанию услуг высокого качества и принятию эффективных управленческих решений;
* повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами компании;
* определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в туристической компании.

Руководители структурных подразделений компании должны обеспечить регулярный контроль за соблюдением положений настоящей Политики, организовать периодические проверки соблюдения информационной безопасности с последующим представлением ежегодного отчета по результатам указанной проверки Руководству.

# **2. Объекты защиты**

Туристическая компания в соответствии с порядком, установленным действующим законодательством РБ, выполняет следующую функцию:

Занимается [продажей](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B4%D0%B0%D0%B6%D0%B0) сформированных [туроператором](https://ru.wikipedia.org/wiki/%D0%A2%D1%83%D1%80%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80) [туров](https://ru.wikipedia.org/wiki/%D0%A2%D1%83%D1%80_(%D0%BF%D1%83%D1%82%D0%B5%D1%88%D0%B5%D1%81%D1%82%D0%B2%D0%B8%D0%B5)). Турагент приобретает туры у туроператора и реализует [туристский продукт](https://ru.wikipedia.org/wiki/%D0%A2%D1%83%D1%80%D0%B8%D1%81%D1%82%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82) покупателю, либо выступает посредником между туристом и туроператором за комиссионное вознаграждение, предоставляемое туроператором.

Организационная структура компании представлена на рисунке 1.

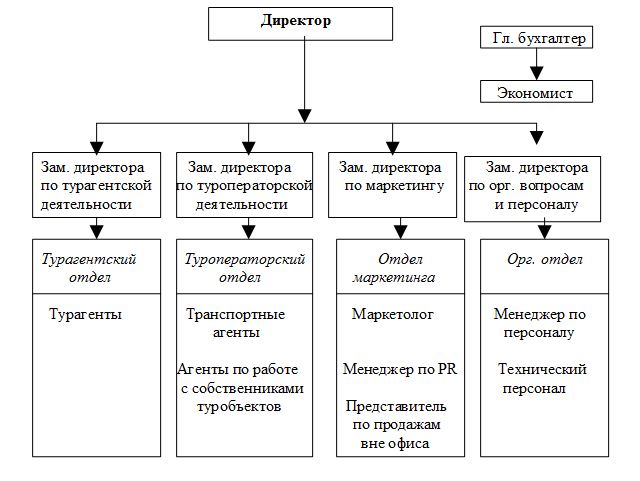


Рисунок 1 – организационная структура туристической компании

Субъекты защиты:

* + Личные данные клиентов (компания работает с паспортными данными клиентов, необходимыми для бронирования и оформления туристических услуг).
  + Финансовые данные компании (документы о счетах компании, договоры между компанией и банками).
  + Веб-сайт компании
  + Внутренние документы компании (документы для внутреннего обращения в компании, документы о сотрудничестве с компаниями-партнёрами).

Объекты защиты:

* + Работники компании (весь персонал и сотрудники компании всех уровней).
  + Компании-партнёры (компании, сотрудничество с которыми необходимо для организации деятельности компании (компании-перевозчики, компании, представляющие интересы отелей и т.д.).
  + Клиенты компании

Подлежащая защите информация хранится как в электронном, так и в бумажном виде на серверах компании, на персональных компьютерах сотрудников отделов и в архиве документов; с информацией работают сотрудники указанных отделов, и, соответственно, только сотрудники отделов имеют доступ к соответствующей информации.

# **3. Основные угрозы и их источники**

Естественные:

Природные катастрофы, последствиями которых является повреждение личного имущества компании

Искусственные:

Угрозы, указанные в пунктах о преднамеренных и непреднамеренных угрозах

* Непреднамеренные:
  + Пожары, произошедшие не по причине поджога
  + Предоставление несанкционированного доступа к информационным ресурсам компании в результате сбоя ПО
* Преднамеренные:
  + Пожары, произошедшие по причине поджога
  + Преднамеренные угрозы информационным ресурсам компании со стороны сотрудников компании или лиц и организаций, не входящих в состав компании
  + Преднамеренные угрозы целостности оборудования компании со сторон сотрудников компании или лиц и организаций, не входящих в состав компании

Внешние:

* Преднамеренные угрозы информационным ресурсам компании со стороны лиц и организаций, не входящих в состав компании
* Преднамеренные угрозы целостности оборудования компании со сторон лиц и организаций, не входящих в состав компании
* Хакерские атаки извне на информационные ресурсы компании

Внутренние:

* Действия сотрудников компании, совершённые умышленно и направленные на нанесение вреда информационным ресурсам компании или оборудованию компании
* Действия сотрудников компании, совершённые неумышленно направленные или повлекшие за собой нанесение вреда информационным ресурсам компании или оборудованию компании
* Сбои программного обеспечения и оборудования

# **4. Оценка угроз, рисков, и уязвимостей**

Анализ ценности ресурсов показал следующее: наиболее ценные ресурсы – личные данные клиентов и банковские данные компании. Ниже по важности идут внутренние документы компании. После них – сайт компании.

Оценка значимости угроз (оценка рисков).

Для оценки значимости угроз, необходимо предварительно составить таблицу условной численной шкалы для оценки финансового ущерба компании (таблица представлена ниже).

Таблица 1. - Условная численная шкала для оценки ущерба

|  |  |
| --- | --- |
| Величина ущерба | описание |
| 0 | Инцидент принесет ничтожный моральный и финансовый ущерб фирме |
| 1 | Ущерб от инцидента есть, но он незначителен, основные финансовые операции и положение компании на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но её положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От компании уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, фирма на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |
| 5 | Компания прекращает существование |

Также необходимо составить вероятностно-временную шкалу реализации угрозы информационным ресурсам (таблица представлена ниже)

Таблица 2. - Вероятностно-временная шкала реализации угрозы

|  |  |
| --- | --- |
| Вероятность события (угрозы) | Средняя частота события (угрозы) |
| 0 | Данный вид угрозы отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Ниже представлена таблица, отображающая результат оценки рисков для компании (значения для граф «Ущерб» и «Вероятность» взяты из таблиц выше).

Таблица 3. – Оценка рисков.

|  |  |  |  |
| --- | --- | --- | --- |
| Описание инцидента | Ущерб | Вероятность | Риск |
| Получение злоумышленником доступа к информационным ресурсам путём внешней атаки | 3 | 0,1 | 0,3 |
| Пожар | 3 | 0,1 | 0,3 |
| Природные катастрофы | 1 | 0,1 | 0,1 |
| Повреждение информационных ресурсов в результате сбоя ПО | 2 | 0,1 | 0,2 |
| Получение злоумышленником доступа к информационным ресурсам путём атаки изнутри компании | 3 | 0,2 | 0,6 |
| Непреднамеренная угроза состоянию оборудования в следствии действий сотрудников компании, не преследующих злого умысла | 1 | 0,3 | 0,3 |
| Преднамеренная угроза состоянию оборудования в следствии действий сотрудников компании, преследующих злого умысла | 4 | 0,1 | 0,4 |
| Преднамеренная угроза состоянию оборудования в следствии действий со сторон лиц и организаций, не входящих в состав компании, преследующих злого умысла | 5 | 0,1 | 0,5 |
| Итого: |  | 1,1 | 2,7 |

Оценка эффективности средств защиты.

Так как итоговые риски численно получились довольно большими, предприятие не может безопасно существовать без изменений в политике безопасности.

**5. Меры, методы и средства обеспечения требуемого уровня защищённости информационных ресурсов**

Считаю необходимым провести следующие мероприятия по снижению рисков для компании:

* + - * Увеличение качества работы с персоналом, повышение информационной грамотности персонала
      * Усиление физической защиты объектов ИВС
      * Использовать антивирусные программы - программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.
      * Установление единого порядка хранения и обращения конфиденциальной информации;
      * Заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности и сохранность конфиденциальной информации;
      * Минимизация данных, доступных работникам. Каждый работник должен знать только те детали процедур, которые необходимы ему для выполнения обязанностей;

# **Выводы и предложения**

В ходе лабораторной работы была разработана политика безопасности для типовой туристической компании, которая работает с большим потоком данных, клиентов и информации, были выявлены при оценочной работе, достаточно серьёзные риски при потере/краже конфиденциальных данных, которые представляют значимую ценность. Также при более глубоком изучении вопроса были выявлены серьёзные последствия утери личных данных клиентов и сотрудников. В итоге были предложены меры по усилению защищённости информационных ресурсов компании.