МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа № 1**

**РАЗРАБОТКА И ВНЕДРЕНИЕ**

**ПОЛИТИКИ БЕЗОПАСНОСТИ**

для туристической компании

Разработала: Некрасова А.П.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

# **Введение**

В нынешнее время все компании нуждаются в информационных технологиях для того, чтобы выдерживать конкуренцию в условиях повсеместного использования высокотехнологичных решений. Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры.

Жизнь современного общества немыслима без информационных технологий. Программные средства обслуживают банковские системы, распределяют энергию, следят за расписанием поездов. Они обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса о разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности.

Высокая степень автоматизации порождает риск снижения личной, информационной и государственной безопасности, делая ее чрезвычайно уязвимой. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, Конституции, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

**Обоснование актуальности**

Любой компании, ведущей свой бизнес, приходится работать с информацией везде и всегда, как при планировании долгосрочных стратегических задач, так и при рутинных канцелярских делах. В процессе бурного развития науки и техники появилось немало методов и средств работы с информацией, порой настолько сложных, что применение их, их адаптация к специфике конкретной компании и условий, в которых она находится, сейчас уже является отдельным классом задач, решаемых специализированными ИТ организациями.

Каждая фирма имеет дело с внешними и внутренними источниками информации, с выполнением таких операций, как сбор информации, ее первичная обработка, отображение, кодирование и декодирование, преобразование, запоминание (хранение), передача, защита. В средних и тем более крупных по размеру компаниях осуществление вышеуказанных операций немыслимо без применения информационных технологий. Под информационными технологиями здесь понимаются: обычные средства; средства на основе вычислительной техники; методы связи.

**Цель ИБ:** обеспечение защиты информации посредством обучения сотрудников и внедрения необходимого программного обеспечения и оборудования.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которые руководство считает целесообразным выделить.

К **задачам** политики информационной безопасности относятся:

* реализация требований законодательства гос-ва в части ИБ информационных систем и мер контроля их защищенности;
* определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований политики конфиденциальности;
* своевременное выявление и оценка причин, условий и характера угроз ИБ и дальнейшее прогнозирование развития событий;
* разработка мер противодействия угрозам;
* реализация программ по осведомленности сотрудников (работников) о возможных рисках угроз ИБ и обучению мерам противодействия.

Туристическая отрасль – одна из самых чувствительных к угрозам информационной безопасности. Это и неудивительно – ведь туристические компании обрабатывает самую разную конфиденциальную информацию о своих клиентах, а даже обыденные сведения о туристе могут сказать очень много о его вкусах, привычках, предпочтениях и состоянии здоровья. Информационная безопасность туристической фирмы может быть обеспечена только при условии строгого соблюдения норм в области защиты персональных данных.

Помимо этого, туризм – одна из отраслей, наиболее часто использующих платежи через интернет. Бронирование номеров в гостиницах, резервирование авиабилетов и другой инфраструктуры с оплатой через Всемирную сеть – самое обычное явление в сфере путешествий и туризма. Поэтому одной из самых важных задач туристических компаний является безопасная обработка банковских данных и реализация всех требований PCI DSS (стандарта защиты данных в индустрии платежных карт).

Информационная безопасность туристической фирмы, как правило, обеспечивается теми же процедурами и средствами, что и любого другого коммерческого предприятия, но с учетом повышенного количества чувствительных данных и транзакций.

**Объекты защиты**

Структура туристических компаний чаще всего выглядит таким образом:

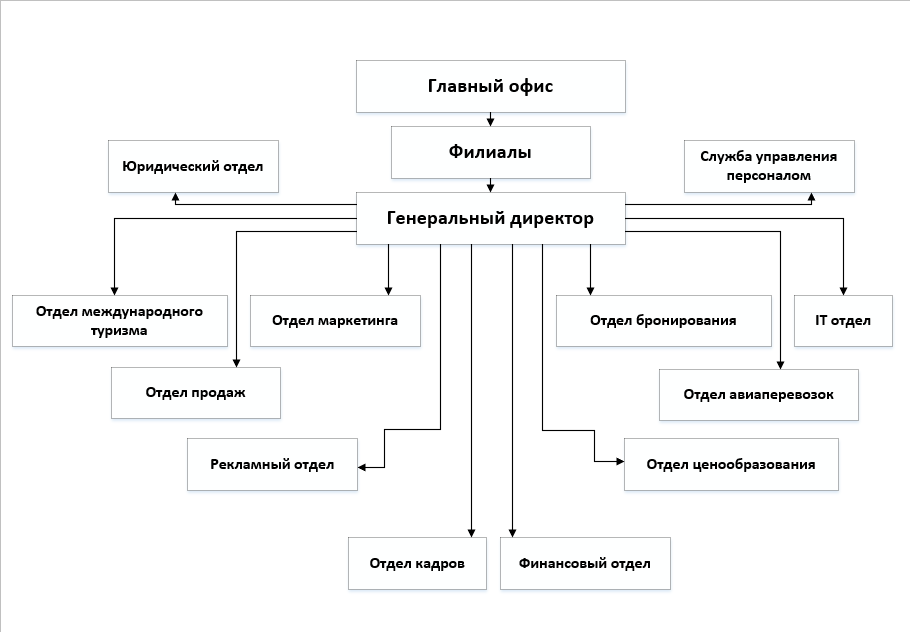


Рисунок 1 – Структура туристической компании

Информационная среда туристической компании является распределенной структурой, объединяющей информационные подсистемы главного офиса, филиалов и представителей, закрепленных за филиалами.

Существует два структурных уровня:

* высшее руководство (дирекция);
* среднее руководство (руководители отделов).

К **объектам** защиты туристической компании относят:

* коммерческая тайна самой туристической компании, данные о ее договорах, финансовых взаимоотношениях, бухгалтерская информация;
* коммерческая тайна клиентов и партнеров организации, данные об их активах, имуществе, платежах, произошедших поездках;
* персональные данные сотрудников компании и сотрудников клиентов, эта информация иногда включает номера автомобилей, водительских удостоверений, кредитных карт;
* медицинская тайна клиентов компании.

Эти данные могут стать объектом противоправного покушения, их сохранность требует принятия серьезных мер безопасности. Несанкционированный доступ к охраняемым законом сведениям является уголовным преступлением, предусмотренным статьей 349 Уголовного кодекса РБ.

В качестве **субъектов** информационных отношений чаще всего выступают клиенты, сотрудники и партнеры компании, компьютер.

**Основные угрозы и их источники**

В зависимости от критерия классификации, угрозы информационной безопасности туркомпании можно условно разделить на следующие основные подтипы:

* естественные и искусственные;
* преднамеренные и непреднамеренные;
* внешние и внутренние.

К *естественным* угрозам относят природные явления, которые не зависят от человека:

* ураганы;
* наводнения;
* пожары;
* возникновение неправильной адресации пакетов.

*Искусственные* угрозы зависят непосредственно от человека. К ним относятся:

* угроза проникновения на рабочие места людей, не являющихся работниками отделов;
* угроза отключения электричества, в связи с недобросовестной работой сотрудников предприятия, что приведет к сбою незавершенных операций и потере данных.

*Непреднамеренные* угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть:

* установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы;
* халатность работников компании;
* ошибки пользователей.

*Преднамеренные* угрозы, в отличии от предыдущих, создаются специально. К ним можно отнести:

* атаки злоумышленников извне
  + фишинг;
  + mailbombing;
  + фарминг;
  + кражи
  + нападения
  + взломы
* атаки злоумышленников изнутри:
  + кража документов;
  + фальсификация данных;
* разглашение сотрудниками конфиденциальной информации.

Наиболее значимыми *источниками угроз* безопасности информации туристической компании являются:

* нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов туристической компании, а также фальсификация (подделка) документов;
* разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
* отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для входа в систему.

**Оценка угроз, рисков и уязвимостей**

Согласно статистике, все туркомпании имеют незакрытые критические уязвимости на ПК и серверах, половина – на сетевом оборудовании. 20% компаний не имеют даже минимальной системы защиты, 40% – уязвимы для действий инсайдеров, а 50% – не защищены от внешних угроз. Причинами являются отсутствие шифрования данных; реагирования на инциденты; неразграниченные права доступа; из всех средств защиты присутствуют лишь антивирус и слабые пароли.

На практике это, в частности, означает высокую вероятность взлома; моментальную доступность конфиденциальной информации при утере или выемке устройства, на которой она хранится; неотслеживаемость действий инсайдеров; невозможность узнать и отреагировать на кибератаку.

В частности, нарушение конфиденциальности данных туркомпании зачастую приводит к вымогательству и шантажу, инсайдерской торговле и недобросовестной конкуренции. Это не только нанесет урон репутации – турфирма понесет ответственность – от финансовой до уголовной.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. При оценивании рисков учитывается:

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами: количественными (например, стоимостными), качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный) или их комбинацией.

Табл. 1 – Условная численная шкала для оценки ущерба туркомпании

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 1 | Раскрытие данных принесет ничтожно малый моральный и экономический ущерб компании |
| 2 | Ущерб от атаки есть, но основные операции и положения затронуты не будут |
| 3 | Значительные финансовые потери и потери доверия со стороны клиента, ощутимая часть которых уйдет |
| 4 | Потери очень значительные, компания теряет свое положение на рынке на период до 3-ух лет. Для восстановления положения потребуются крупные финансовые займы |
| 5 | Компания прекращает существование |

В таблице 1 показаны последствия различной величины ущерба

Можно конкретизировать определение вероятности наступления угрозы ресурсу. Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка ПБ требует учета специфики туркомпании. На таблице 2 приведена шкала вероятности того, что угроза будет реализована.

Табл. 2 – Вероятностно-временная шкала реализации НСД к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,3 | Около 1 раза в год |
| 0,5 | Около 1 раза в месяц |
| 0,8 | Около 1 раза в неделю |
| 1 | Практически ежедневно |

Также можно создать таблицу рисков, на этапе анализа которой риски задаются некоторым максимально допустимым уровнем (порогом). Далее проверятся каждая строка таблицы: превышен или не превышен порог для значения риска, связанного с анализируемой атакой.

Табл. 3 – Оценка рисков

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Атака** | **Ущерб** | **Вероятность** | **Риск возникновения** |
| 1 | Природные явления: пожар, наводнение, ураган, … | 4 | 0,1 | 0,4 |
| 2 | Проникновение на рабочее место человека, не являющегося сотрудником | 4 | 0,1 | 0,4 |
| 3 | Халатность сотрудников | 3 | 0,5 | 1,5 |
| 4 | Ошибки пользователей | 2 | 1 | 2 |
| 5 | Установка вредоносного ПО на офисное оборудование | 3 | 0,3 | 0,9 |
| 6 | Кражи, нападения, взлом, саботаж и проникновение (физические) | 4 | 0,1 | 0,4 |
| 7 | Кражи, проникновения (виртуальные) | 3 | 0,8 | 2,4 |
| 8 | Фарминг (перенаправление на фейковый ip) | 1 | 0,8 | 0,8 |
| 9 | Mailbombing | 2 | 0,5 | 1 |
| 10 | Фишинг  (получ. доступа к конфид. данным пользов.) | 4 | 0,3 | 1,2 |
| 11 | Копирование архивных данных | 3 | 0,1 | 0,3 |
| 12 | Фальсификация данных сотрудниками | 3 | 0,3 | 0,9 |
|  | **Итого** |  |  | **12,2** |

Если такое превышение имеет место, данная атака должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности (таблица 3).

**Разработка мер защиты**

Информационная безопасность туркомпаниидолжна обеспечиваться целым комплексом мер, среди которых:

* административно-правовые;
* организационные;
* программно-технические.

Данные меры следует применять совместно. Опираться система защиты должна на управление персоналом компании и контроль над ним. Меры технического характера не менее важны, но не могут существовать в отрыве от организационных мер.

*Административные* меры безопасности включают в себя разработку внутренних нормативных документов, обеспечивающих информирование сотрудников о системе действий, необходимых для обеспечения информационной безопасности. В туркомпании должно быть организовано ознакомление персонала с внутренними нормативными документами.

Все трудовые договоры должны содержать перечень информации, носящей характер коммерческой, а в самих договорах должны быть предусмотрены меры ответственности за ее разглашение.

*Организационные* меры безопасности направлены на устранение внутренней угрозы утечки информации и мотивацию сотрудников на соблюдение утвержденных регламентов. Эти меры предпринимаются службой безопасности во взаимодействии с сотрудниками служб управления персоналом.

Иногда система работы с безопасностью информации требует создания в компании специального подразделения, в чьи функции будет входить только эта деятельность.

*Технические* меры рассчитаны на использование действенных технических средств защиты. Для их реализации используются аппаратные, программные и криптографические средства. Первые предполагают установку систем резервного копирования и защиту от несанкционированного проникновения, вторые отвечают за работу антивирусов и иных защитных программ, третьи обеспечивают шифрование всей хранимой и передаваемой по каналам связи информации. Наиболее часто для защиты информации применяются межсетевые экраны и системы обнаружения вторжений. Технические средства требуют постоянного обновления и модернизации, так как скорость устаревания программных продуктов очень высока.

Комплексное применение современных технических средств в работе службы безопасности туркомпании может обеспечить высокий уровень защиты информации от утечек и несанкционированного доступа.

В таблице 4 представлены конкретные меры защиты, организованные против угроз из таблицы 3.

Табл. 4 – Меры защиты

|  |  |
| --- | --- |
| **Атака** | **Мера защиты** |
| Природные явления: пожар, наводнение, ураган, … | Экстренная связь офиса с МЧС, милицией и пожарной службой (наличие кнопок экстренного вызова);  Четкий инструктаж персонала на случай чрезвычайного происшествия. |
| Проникновение на рабочее место человека, не являющегося сотрудником | Наличие охраны;  Наличие системы видеонаблюдения;  Наличие пропускной системы с удостоверением личности для рабочего персонала. |
| Халатность сотрудников | Чёткие обязанности каждого сотрудника в части доверенной ему работы;  Обеспечение комнат отдыха;  Минимизация давления на сотрудников со стороны вышестоящих. |
| Ошибки пользователей | Квалифицированный IT-отдел;  Простой и нативно понятный интерфейс;  Большое количество всевозможной валидации в приложении. |
| Установка вредоносного ПО на офисное оборудование | Квалифицированный IT-отдел;  Меры ответственности за нарушение положений; |
| Кражи, нападения, взлом, саботаж и проникновение (физические) | Наличие охраны;  Наличие системы видеонаблюдения;  Наличие пропускной системы с удостоверением личности для рабочего персонала. |
| Кражи, проникновения (виртуальные) | Подготовка решений по обеспечению конфиденциальности, доступности, целостности данных;  Привлечение к ответственности лиц, виновных в разглашении информации; |
| Фарминг (перенаправление на фейковый ip) | Использовать защиту электронного почтового ящика (отключить предварительный просмотр);  Не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов. |
| Mailbombing | Давать адрес электронной почты только проверенным источникам. |
| Фишинг  (получ. доступа к конфид. данным пользов.) | Использовать только проверенные ресурсы и пути доступа к ним. |
| Копирование архивных данных | Больше внимания уделить защите этих данных;  Контроль за действиями администраторов баз данных, серверов и сетевых устройств;  Принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;  Привлечение к ответственности лиц, виновных в разглашении информации; |
| Фальсификация данных сотрудниками | Привлечение к ответственности лиц, виновных в разглашении информации; |

**Вывод**

Мною были выявлены все возможные угрозы и их источники информационной безопасности в туркомпании, а также проанализированы и оценены собранные данные.

На основании этого была разработана концепция и основные элементы политики безопасности для туркомпании.

Также были разработаны мероприятия по внедрению разработанной мной политики безопасности на предприятии.

Результаты проделанной работы оформлены в виде описания разработанной политики безопасности, а также плана мероприятий по ее реализации.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки, можем выделить следующие рекомендации, следуя которым возможно снизить риски опасного воздействия и их последствий:

* четкая и строгая иерархия должностей и полномочий в компании; каждый должен заниматься строго своим заданием;
* обязательная экстренная связь офиса с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, баз данных милиции;
* защита серверов компании и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файрволлы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие в офисе наглядного отображения плана по работе во время чрезвычайных ситуаций.