Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Разработка и внедрение политики безопасности туристической компании

Студент: Коломейчук А. А.
ФИТ 3 курс 6 группа
Преподаватель: Блинова Е. А.

Содержание

Введение

Защита информации является критически важной для обеспечения конфиденциальности, целостности и доступности данных в туристической компании. В современном мире, когда информация передается и хранится в цифровом формате, угрозы безопасности стали более распространёнными. Несанкционированный доступ к конфиденциальной информации может привести к утечке личных данных клиентов, финансовым потерям и разрушению репутации компании. Чтобы избежать столь серьёзных последствий и обеспечить защиту информации, необходима разработка политики информационной безопасности.

Разработка политики информационной безопасности является одной из ключевых задач для любой успешной туристической компании. Это особенно важно, так как компании приходится работать с большим объёмом информации, включающей в себя персональные данные клиентов и корпоративные данные. К таким данным относятся:

– информация о клиентах (ФИО, контактные данные, паспортные данные, данные о поездках, предпочтения и прочее);

– финансовые данные (оплаты, бронирования, бухгалтерская отчетность и прочее).

Исходя из этого, можно выделить следующие цели и задачи разработки ПИБ:

Цели:

– обеспечение конфиденциальности информации;

– предотвращение утечек данных;

– защита от вирусов и вредоносного ПО;

– соответствие нормативным требованиям, установленным законодательством.

Задачи:

– описание структуры компании и её информационных систем;

– выявление уязвимостей и рисков информационной безопасности компании;

– оценка вероятности возникновения угроз и потенциального ущерба от них;

– разработка мер, методов и средств обеспечения необходимого уровня защищенности информации в компании;

– разработка процедур и инструкций по обеспечению информационной безопасности компании.

1 Объекты защиты

1.1 Описание структуры организации

Рассмотрим структуру туристической компании. Она представляет собой иерархическую организацию, в которой выделяются несколько уровней управления.

Руководство компании. Этот уровень представлен генеральным директором компании, который является главным руководителем организации и несет ответственность за ее деятельность перед советом директоров и акционерами. Он управляет деятельностью всех подразделений компании и принимает стратегические решения.

Отдел продаж и обслуживания клиентов. Отвечает за поиск и привлечение новых клиентов, а также за обслуживание текущих клиентов. Он занимается разработкой и продажей туристических пакетов, бронированием туров, авиабилетов, гостиниц и других услуг. Этот отдел также обрабатывает запросы и претензии клиентов, предоставляя им необходимую поддержку.

Отдел маркетинга. Занимается маркетинговыми исследованиями, разработкой маркетинговых стратегий, рекламой и продвижением услуг компании. Он анализирует рыночные тенденции, разрабатывает рекламные кампании, создает контент для социальных сетей и проводит мероприятия для привлечения клиентов.

Отдел бронирования и логистики. Отвечает за управление бронированиями, координацию туров, разработку маршрутов и логистическую поддержку. Он взаимодействует с партнерами, такими как авиакомпании, отели, транспортные компании и экскурсионные бюро, для обеспечения качественного обслуживания клиентов.

Финансовый отдел. Отвечает за финансовое планирование и анализ, управление бухгалтерской отчетностью, управление рисками и обеспечение финансовой стабильности компании. Он контролирует доходы и расходы, разрабатывает бюджеты и финансовые отчеты, а также анализирует финансовые показатели компании.

Юридический отдел. Обеспечивает юридическую поддержку компании, обрабатывает договоры, участвует в переговорах с партнерами и клиентами, а также занимается вопросами лицензирования и соответствия законодательным требованиям.

IT-отдел. Отвечает за информационные технологии компании, включая разработку и поддержку информационных систем, сетевой инфраструктуры, безопасности и обеспечения бесперебойной работы информационно-вычислительных систем. Он также занимается разработкой и поддержкой веб-сайта компании и онлайн-платформ для бронирования туров.

Отдел кадров. Занимается наймом, обучением и управлением персоналом компании. Он разрабатывает и внедряет политику компании в области управления персоналом, включая оплату труда, стимулирование и

мотивацию сотрудников, а также обеспечивает их профессиональное развитие.

Отдел управления проектами. Отвечает за планирование, контроль и управление проектами компании. Он состоит из проектных менеджеров и команд, которые занимаются реализацией различных проектов, связанных с развитием компании и улучшением качества предоставляемых услуг.

Отдел контроля качества. Занимается контролем и обеспечением качества услуг, предоставляемых компанией. Он анализирует обратную связь от клиентов, проводит внутренние аудиты и разрабатывает меры по улучшению качества обслуживания.

Взаимодействие отделов. Каждый отдел имеет своего руководителя, который отчитывается перед генеральным директором компании. Все отделы взаимодействуют друг с другом и координируют свои действия для достижения общих целей компании, обеспечивая высокое качество обслуживания клиентов и эффективность работы.

1.2 Объекты ИВС

В туристической компании можно выделить следующие объекты информационно-вычислительной системы, которые необходимо защищать:

– сеть;
– серверы;
– сетевые ресурсы;
– системы бронирования и управления турами;
– электронная почта;
– системы управления клиентскими отношениями;
– базы данных.

В целом, объекты ИВС для туристической компании включают в себя все устройства и системы, которые используются для обработки, хранения, передачи и управления информацией.

1.3 Субъекты ИВС

Защищать необходимо не только различные источники информации, но и тех, кто может этими объектами воспользоваться. В туристической компании можно выделить следующие субъекты, требующие обеспечения информационной безопасности:

– сотрудники компании, а также устройства, которые они используют;
– рабочие станции, которыми пользуются сотрудники;
– администраторы ИВС, которые управляют сетевой инфраструктурой, настраивают программное обеспечение и обеспечивают безопасность системы;
– клиенты, которые предоставляют конфиденциальные данные туристической компании для бронирования туров и других услуг;

– партнеры и поставщики, которые имеют доступ к информации о бизнес–процессах и технологиях компании;

– злоумышленники, которые могут попытаться получить несанкционированный доступ к информации или навредить системе;

– государственные органы и регуляторы, которые могут потребовать доступ к информации компании в соответствии с законодательством.

Все эти субъекты могут оказать влияние на безопасность ИВС и требуют соответствующих мер по защите информации.

2 Основные угрозы и их источники

2.1 Естественные угрозы

Естественные угрозы для туристической компании можно разделить на три категории:

– погодные явления: к этой категории относятся наводнения, пожары, ураганы, сильные ветры и т.д. Эти явления могут привести к разрушению зданий и инфраструктуры, прерыванию электроснабжения и связи, а также к потере оборудования и данных.

– климатический кризис: в эту категорию входят частые и сильные экстремальные погодные явления, вызванные глобальным потеплением, такие как наводнения, лесные пожары и т.д. Это может привести к непредсказуемым последствиям для работы компании, включая снижение потока туристов и потери данных.

– геологические процессы: к этой категории относятся землетрясения, извержения вулканов и сейсмические деформации, которые могут привести к нарушению работы инфраструктуры компании, а также к потере данных.

В целом, для защиты от естественных угроз необходимо проводить оценку рисков и разрабатывать соответствующие планы, чтобы быстро восстановить работу компании в случае возникновения чрезвычайной ситуации. Также важно обеспечить безопасность данных и резервное копирование информации для предотвращения её потери в результате естественных катастроф.

2.2 Искусственные угрозы

Искусственные угрозы – это угрозы, связанные с использованием современных технологий и информационных систем, которые могут привести к нарушению безопасности компьютерных систем, сетей и данных, а также к различным видам мошенничества, кражи личных данных, финансовых потерь и т.д.

Туристическая компания может столкнуться с различными видами искусственных угроз. Ниже приведены возможные виды угроз, которые могут возникнуть, а также категории, к которым они могут быть отнесены:

– кибербезопасность: взлом компьютерных систем, кража конфиденциальных данных, фишинг, распространение вредоносных программ;

– конкуренция: нарушение авторских прав, незаконное использование технологий, похищение персонала, подделка удостоверений компании;

– финансы: кража финансовых данных, мошенничество при проведении платежей, сбои в системах онлайн–банкинга, незаконное снятие денежных средств со счетов компании;

– репутация: негативные отзывы в социальных сетях, распространение ложной информации, утечки конфиденциальных данных клиентов, неправильное представление компании в СМИ;

– регуляторные вопросы: нарушения в области защиты данных, несоблюдение правил и норм, установленных регулирующими органами, неправильное оформление документации, незаконное использование конфиденциальной информации;

– физические и инфраструктурные угрозы: незапланированные перебои в подаче электроэнергии, незапланированные перебои в работе сети, ограбление.

2.3 Преднамеренные угрозы

Преднамеренные угрозы могут быть вызваны многими факторами, включая мотивацию для получения выгоды, политические или идеологические мотивы, или просто желание нанести вред. Независимо от мотивации, результатом таких угроз могут быть утечки данных, нарушения безопасности и повреждения информационно-вычислительных систем.

Конкретными примерами таких угроз для туристической компании являются:

– кража конфиденциальной информации: сотрудники компании могут украсть или скопировать конфиденциальную информацию клиентов, чтобы продать её конкурентам или использовать в личных целях;

– несанкционированный доступ к системам: сотрудники могут использовать свои привилегии для доступа к информации, которая не относится к их работе, или использовать несанкционированные способы доступа к системам;

– вредоносные действия: сотрудники могут внедрять вредоносные программы на компьютеры и сети компании, чтобы получить доступ к конфиденциальной информации или нарушить работу систем;

– саботаж: сотрудники могут наносить ущерб системам и сетям компании, чтобы причинить ущерб её бизнесу;

– утечки данных: сотрудники могут неосторожно раскрыть конфиденциальную информацию или утечки могут происходить вследствие несанкционированных действий.

Все эти угрозы могут привести к серьёзным последствиям для туристической компании, таким как утечка конфиденциальной информации, нарушение законодательства, потеря доверия клиентов и репутации, а также финансовые потери.

2.4 Непреднамеренные угрозы

В дополнение к преднамеренным угрозам, туристические компании должны учитывать и непреднамеренные. Они, в свою очередь, могут быть

вызваны различными факторами, такими как человеческий, технический, природный и внешний.

Ниже рассмотрим конкретные примеры:

– человеческий фактор: ошибки и недостатки персонала, например, неправильное использование программного обеспечения, нарушение процедур безопасности, утеря данных, неправильная обработка и передача информации;

– технический фактор: сбои в аппаратной или программной части, возникшие вследствие естественных причин, таких как сбой оборудования, неправильная установка и настройка оборудования;

– природные катастрофы: пожары, наводнения, землетрясения, ураганы и другие стихийные бедствия, которые могут привести к потере данных и нарушению функционирования информационной системы;

– внешние атаки: к компьютерным системам могут направляться атаки со стороны злоумышленников с целью получения конфиденциальной информации или нарушения работы системы.

Для того чтобы защититься от непреднамеренных угроз, необходимо внедрить соответствующие меры безопасности, такие как контроль доступа, системы резервного копирования и восстановления данных, защиту от вредоносных программ и др.

2.5 Внешние угрозы

Внешние угрозы – это различные факторы, события и процессы, которые находятся за пределами компании и могут негативно повлиять на её бизнес-операции, финансовые показатели и репутацию.

Для туристической компании внешние дестабилизирующие факторы могут быть следующими:

– угрозы безопасности информации: неквалифицированные пользователи, несанкционированный доступ к информационным системам с целью модификации данных, угрозы кибербезопасности (хакерские атаки, вирусы, фишинг и другие мошеннические схемы);

– угрозы природного характера: внешние климатические условия, неблагоприятные природные явления;

– технические угрозы: электромагнитные и ионизирующие помехи, перебои в электроснабжении;

– угрозы социально–психологического характера: нарушение этики и профессионального поведения сотрудников, которое может негативно сказаться на репутации и имидже компании.

2.6 Внутренние угрозы

Внутренние угрозы – это различные факторы, связанные с деятельностью и поведением внутри компании, которые могут негативно повлиять на её бизнес–операции, финансовые показатели и репутацию.

К внутренним угрозам для туристической компании относятся:

– нарушение правил доступа и безопасности информации сотрудниками компании: нарушение политики паролей, отсутствие многофакторной аутентификации, неправомерный доступ к конфиденциальной информации, несанкционированное использование учетных данных других сотрудников;

– недостаточная безопасность сети и инфраструктуры: несанкционированный доступ к сетевым ресурсам, уязвимости в системах защиты, отсутствие мониторинга сети и обнаружения инцидентов, неправильная конфигурация сетевых устройств;

– неправомерное использование корпоративных ресурсов: использование компьютеров и сети компании для личных целей, работа с конфиденциальной информацией клиентов, нарушение правил использования программного обеспечения;

– нарушение процедур безопасности при обработке и хранении конфиденциальной информации: отсутствие шифрования данных, неправильное хранение паролей и другой конфиденциальной информации, небезопасная передача конфиденциальной информации по сети, несанкционированный доступ к конфиденциальной информации.

Туристические компании должны принимать меры по защите своих систем, клиентов и данных, чтобы избежать возможных угроз. Это может включать в себя использование современных методов шифрования данных, установку многофакторной аутентификации и регулярную проверку наличия уязвимостей в системах. Кроме того, компании должны иметь стратегию по реагированию на угрозы и четкий план действий в случае возникновения проблем.

3 Оценка угроз, рисков и уязвимостей

Чтобы оценить возможный ущерб, который может быть нанесён туристической компании, воспользуемся шкалой для численной оценки рисков от несанкционированного доступа (НСД) к информационным ресурсам туристической компании. В данной шкале каждой степени ущерба присваивается число от 1 до 5. Числовые значения для оценки ущерба и соответствующие им описания представлены в таблице 3.1.

Таблица 3.1 условная численная шкала для оценки ущерба компании

Величина ущерба	**Описание**
0	Раскрытие информации принесет ничтожный моральный и финансовый ущерб туристической компании
1	Ущерб от атаки есть, но он незначителен, финансовое положение, а также положение туристической компании на рынке не нарушены
2	Финансовые операции не ведутся в течение некоторого времени, за это время туристической компания терпит убытки, но её положение на рынке и количество клиентов изменяются минимально
3	Значительные финансовые потери, а также потери на рынке. Также ощущаются потери в виде клиентов.
4	Потери очень значительные, туристической компания теряет своё положение на рынке. Многие клиенты прекращают своё сотрудничество с компанией. Требуются крупные финансовые затраты для восстановления былого положения.
5	Туристической компания прекращает своё существование

Пример создания шкалы вероятности того, что угроза будет реализована, приведен в таблице 3.2.

Таблица 3.2 вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

Вероятность события	**Средняя частота события (НСД)**
0	Данный вид атаки 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

Далее, на основании таблиц 3.1 и 3.2 можно составить таблицу рисков. На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем. В данном случае это значение 0.5.

Таблица 3.3 оценка рисков

Описание атаки	**Ущерб**	**Вероятность**	**Риск**
Фишинг (выманивание паролей)	4	0,4	1,6
Взлом информационной системы	5	0,3	1,5
Использование уязвимости в системе безопасности	4	0,3	1,2
Перехват и анализ трафика	3	0,3	0,9
Утечка данных	3	0,3	0,9
SQL-инъекция	4	0,2	0,8
Вредоносное ПО	4	0,2	0,8
DDoS-атака	2	0,4	0,8
Несанкционированный доступ к файлам	2	0,3	0,6
Кража/уничтожение оборудования	5	0,1	0,5
Сбои и отказы оборудования	2	0,2	0,4
Спам	1	0,4	0,4
Отключение электроэнергии	2	0,2	0,4
Обман персонала	2	0,1	0,2
		ИТОГО:	**11,4**

Если интегральный риск превышает допустимый уровень, значит, в системе безопасности набирается множество мелких проблем, которые также нужно решать комплексно. В этом случае из строк таблицы (типов атак) выбираются те, которые «дают» самый значительный вклад в значение интегрального риска. Производится работа по снижению их влияния или полному устранению.

Просматривая таблицу, мы видим, что все описанные интегральные риски не превышают допустимый уровень, что хорошо для компании.

Таким образом, можно сделать вывод, что система безопасности туристической компании нуждается в доработке. И в первую очередь нужно проработать те угрозы безопасности, которые в таблице получили наибольшую оценку риска. А затем уже все остальные.

Взлом информационной системы.

Законодательные меры:

– соблюдение требований законодательства в области информационной безопасности.

Организационные меры:

– обучение сотрудников правилам безопасности;

– проведение аудитов на предмет уязвимостей.

Технические меры:

– применение сложных паролей;

– использование двухфакторной аутентификации или многофакторной аутентификации;

– регулярное обновление систем безопасности.

Фишинг.

Законодательные меры:

– соблюдение законодательства по защите персональных данных и борьбе с киберпреступлениями.

Организационные меры:

– обучение сотрудников правилам безопасности.

Технические меры:

– использование программ и систем, фильтрующих спам;

– применение двухфакторной аутентификации или многофакторной аутентификации;

– проверка ссылок на подозрительные домены и сайты.

Использование уязвимости в системе безопасности.

Законодательные меры:

– соблюдение требований законодательства в области защиты информации.

Организационные меры:

– проведение аудитов на предмет уязвимостей.

Технические меры:

– регулярное обновление программного обеспечения и систем безопасности;

– использование антивирусных программ, фильтрующих вредоносное ПО и уведомляющих о возможных угрозах.

Методы противодействия всем видам атакам описаны в главе 4.

4 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

Для обеспечения должного уровня защиты информационных ресурсов туристической компании необходимо применять соответствующие меры, методы и средства защиты.

Ниже приведены угрозы, представляющие опасность для туристической компании, а также способы защиты от них:

– взлом информационной системы: применение сложных паролей, использование двухфакторной аутентификации или многофакторной аутентификации, регулярное обновление систем безопасности, проведение аудитов на предмет уязвимостей, обучение сотрудников правилам безопасности;

– фишинг: обучение сотрудников правилам безопасности, использование программ и систем, фильтрующих спам, применение двухфакторной аутентификации или многофакторной аутентификации, проверка ссылок на подозрительные домены и сайты;

– использование уязвимости в системе безопасности: регулярное обновление программного обеспечения и систем безопасности, проведение аудитов на предмет уязвимостей, использование антивирусных программ, фильтрующих вредоносное ПО и уведомляющих о возможных угрозах;

– отключение электроэнергии: резервирование электроснабжения, использование генераторов и источников бесперебойного питания, перемещение систем на другой объект в случае длительных отключений;

– обман персонала: обучение сотрудников правилам безопасности, ограничение доступа к конфиденциальной информации, применение двухфакторной аутентификации, контроль действий сотрудников;

– сбои и отказы оборудования: регулярное техническое обслуживание и обновление оборудования, использование резервных систем, быстрое реагирование на возможные сбои и отказы;

– DDoS–атака: использование систем защиты от DDoS–атак, мониторинг сети на предмет аномальной активности, настройка брандмауэра и других систем безопасности для предотвращения атак;

– ошибки эксплуатации оборудования: обучение сотрудников правильной эксплуатации оборудования, регулярное техническое обслуживание и обновление оборудования, использование инструкций и руководств для обслуживания оборудования;

– утечка данных: использование систем защиты данных, ограничение доступа к конфиденциальной информации, шифрование данных, проведение аудитов на предмет утечек;

– вредоносное ПО: использование антивирусных программ, регулярное обновление систем безопасности, запрет на установку непроверенного программного обеспечения;

– SQL–инъекция: использование систем защиты от SQL–инъекций, применение подготовленных запросов к базе данных, фильтрация пользовательского ввода;

– перехват и анализ трафика: использование систем защиты от перехвата и анализа трафика, шифрование данных, использование защищенных протоколов связи;

– кража/уничтожение оборудования: использование систем видеонаблюдения и контроля доступа, физическая защита оборудования, контроль доступа к помещениям;

– спам: использование систем фильтрации спама, обучение сотрудников правилам безопасности, использование проверенных почтовых сервисов и программ.

Применение этих мер и методов поможет снизить вероятность возникновения угроз и обеспечить защиту информационных ресурсов туристической компании от несанкционированного доступа и других видов атак.

Выводы и предложения

Разработанная политика безопасности для туристической компании включает в себя следующие ключевые аспекты:

– оценка и управление рисками: туристическая компания должна регулярно проводить оценку рисков и угроз для информационных систем и данных. Это поможет своевременно выявлять потенциальные уязвимости и принимать меры по их устранению;

– комплексные меры защиты: для обеспечения безопасности информации необходимо применять комплексные меры защиты, включая шифрование данных, использование двухфакторной аутентификации, установку антивирусного ПО и проведение регулярных аудитов безопасности;

– обучение персонала: обучение сотрудников правилам безопасности и методам защиты информации является важным шагом в предотвращении инцидентов. Сотрудники должны быть осведомлены о возможных угрозах и уметь правильно реагировать на них;

– резервное копирование данных: регулярное резервное копирование данных позволит обеспечить их сохранность и восстановление в случае утраты или повреждения;

– реагирование на инциденты: туристическая компания должна иметь план реагирования на инциденты, включая действия по ликвидации последствий атак и восстановлению нормальной работы систем.

Следующие предложения помогут увеличить эффективность политики безопасности, а также улучшить безопасность системы:

– регулярные аудиты безопасности: проводить регулярные аудиты безопасности для выявления и устранения уязвимостей в информационных системах компании;

– обновление программного обеспечения: обеспечить регулярное обновление всех программных и аппаратных средств для защиты от новых угроз и уязвимостей;

– шифрование данных: внедрить системы шифрования данных для защиты конфиденциальной информации клиентов и компании;

– мониторинг сетевой активности: установить системы мониторинга сетевой активности для обнаружения подозрительных действий и предотвращения атак;

– обучение и тренинги: организовывать регулярные тренинги и семинары для сотрудников по вопросам информационной безопасности и методам защиты данных;

– разработка и тестирование плана реагирования: создать и регулярно тестировать план реагирования на инциденты для оперативного решения проблем и минимизации последствий атак;

– контроль доступа: ограничить доступ к конфиденциальной информации только тем сотрудникам, которые непосредственно работают с ней, и применять системы контроля доступа.