Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информатики и веб-дизайна**

**Лабораторная работа №1**

Разработка политики безопасности event-компании

Выполнил:

Студент 3 курса 6 группы ФИТ

Булавский Кирилл Серегеевич

# Обоснование актуальности, цели и задачи разработки ПИБ в организации

Политика информационной безопасности (ПИБ) организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

В современной быстроменяющейся глобальной среде индустрия организации мероприятий сильно пострадала от растущего распространения Интернета и технологических достижений, особенно в областях оптимизации производительности, предложения продуктов и услуг.

Поскольку организаторы мероприятий сосредоточены на улучшении общего впечатления своих посетителей, эта желанная цель привела к частому внедрению технологий для помощи в сборе ценных данных. Компании все больше и больше интересуются информацией, касающейся их участников, мест проведений мероприятий, их воздействия на социальные сети и т. д.

**Цель:** разработать эффективную политику информационной безопасности event-агентства.

**Задачи:**

1. Выделить и классифицировать особенности информационной или информационно-вычислительной системы event-агентства как объекта защиты.

2. Обеспечить необходимый уровень защиты информации в ИВС.

3. Проанализировать угрозы информационной безопасности ИВС.

4. Выделить все возможные угрозы и их источники информационной безопасности агентства, проанализировать и оценить собранные данные.

5. Разработать концепцию, основные элементы политики безопасности для event-агентства.

6. Разработать мероприятия по внедрению предложенной политики безопасности.

7. Результаты оформить в виде описания разработанной политики безопасности, а также плана мероприятий по ее реализации.

# Объекты защиты

Event-агентство – это тип организации, состоящей из группы людей, задача которых состоит в том, чтобы организовывать мероприятия и заботиться о проектировании, планировании и управлении этими мероприятиями для своих клиентов. Компания состоит из нескольких уровней, и исходя из этого, должности делятся на многочисленные категории. В зависимости от размера компании структура иерархии может меняться, но большинство крупных компаний более или менее состоят из одной и той же лестницы должностей.

Позиция *директора* является наиболее важной. Позиция занимает верхнее положение на иерархической диаграмме организации. Директор несет ответственность за руководство и обеспечение бесперебойного функционирования всего мероприятия. В подчинении директора находятся следующие отделы:

*1) Отдел координации программы мероприятия*

Это отдел, который следит за координацией мероприятия и следит за тем, чтобы все, от церемоний до подведения итогов, проходило в плавном порядке и надлежащей последовательности. У него есть несколько других должностей, указанных ниже:

* Координатор мероприятия
* Планировщик событий
* Компьютерный специалист
* Церемониальный менеджер
* Программист-координатор

*2) Отдел координации объектов*

В этом отделе на высшем уровне находится координатор объекта, который занимается такими задачами, как экологический контроль, управление рисками, команда по настройке и бронирование места. Также в отделе работают:

* Управляющий рисками
* Менеджер по бронированию
* Специалист по подбору команды
* Менеджер по поиску волонтеров
* Волонтеры

*3) Творческий отдел*

Отвечает за создание концепций мероприятия и другого креатива. Отдел возглавляет один или несколько креативных директоров. Также в отделе работают:

* Копирайтеры
* Режиссеры
* Сценаристы

*4) Производственный отдел*

Дизайнеры, специалисты по производству. Люди, помогающие воплотить идею, рожденную в креативном отделе. Сюда же относятся фотографы, видеографы и другие специалисты. Менеджеры этого отдела заказывают услуги подрядчиков event-агентства.

*5) Отдел координации оборудования*

Поскольку проведение мероприятия невозможно без многих типов оборудования, более крупные компании по организации мероприятий используют целые отделы для ухода за оборудованием, таким как звуковое оборудование, транспортное оборудование и оборудование для обслуживания. В отдел входят:

* Звуковой менеджер
* Транспортный менеджер
* Водитель
* Уборщик
* Музыканты
* Танцоры

*6) Отдел по продвижению*

Поскольку мероприятие нуждается в рекламе и продвижении, на отдел продвижения возлагаются задачи, связанные с рекламой, связью со СМИ, подборками материалов для СМИ и промо-мероприятиями.

* Координатор продвижения
* Менеджер по рекламе
* Менеджер по маркетингу
* Медиа-эксперт
* Эксперт по продажам
* Директор по продажам
* Руководитель отдела маркетинга

*7) Отдел организации гостеприимства*

Гостеприимство - важная часть любого мероприятия, и для этого более крупные компании используют отделы по координации гостеприимства, чтобы заботиться о приеме, проживании, питании гостей мероприятий.

* Поставщик
* Спонсорский руководитель
* Заведующий больницей

*8) Отдел координации мерчандайзинга*

Еще один отдел, входящий в состав компании по организации мероприятий, это отдел координации мерчандайзинга. Этот отдел выполняет задачи, связанные с продажами, розыгрышами, оснащением волонтеров.

* Менеджер по мерчандайзингу

# Основные угрозы и их источники

**Утечка данных**

Поскольку профессиональные организаторы мероприятий сосредоточены на улучшении общего впечатления для своих посетителей, эта желанная цель привела к частому внедрению технологий для помощи в сборе ценных данных. Компании все больше и больше интересуются информацией, касающейся профилей их участников, места проведения и местоположения, воздействия на социальные сети, отзывы и т. д.

В наши дни индустрия организации мероприятий использует технологии для различных целей. Существует множество инструментов, которые облегчают вашу жизнь. Например, существуют онлайн-формы, которые позволяют собирать данные о посетителях через социальные сети. Вы можете использовать биллинговые системы, которые отправляют счета поставщикам.

Существует возможность онлайн-продажи билетов, которая значительно снижает рабочую нагрузку. Однако самая большая проблема с технологиями и социальными сетями заключается в том, что необходимо собирать конфиденциальные данные. Например, система онлайн-продажи билетов потребует оплату с кредитной карты участника.

Существуют и другие типы информации, которые делают мероприятия отличной целью для киберпреступников. Несанкционированный доступ к этим данным создает множество проблем, которые могут выставить конференцию или сетевое мероприятие в негативном свете.

**Кража личного имущества**

Когда на мероприятиях собирается большое количество людей, воры, к сожалению, видят в этом прекрасную возможность украсть частную собственность. Из-за большого скопления людей они могут совершать самые разные преступные действия, которые остаются незамеченными. К тому же на мероприятиях может быть много дорогих гаджетов.

**Насильственные преступления**

Вероятность насильственных преступлений на мероприятиях довольно мала, однако вам все равно нужно убедиться, что они не имеют места на ваших мероприятиях. Когда ваше мероприятие посещают высокопоставленные или особенные гости, вам необходимо принять дополнительные меры для их защиты. Будут люди, которые хотят навредить этим людям по разным личным причинам.

**Стихийные бедствия**

Несмотря на то, что шансы столкнуться со стихийными бедствиями, такими как пожары, землетрясения и штормы, довольно низки, нельзя их исключать. Они наносят значительный ущерб.

Также стоит отметить ошибки пользователей и системных администраторов; нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации; ошибки в работе программного обеспечения; отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

Формами проявления внешних угроз являются:

Заражение компьютеров вирусами или вредоносными программами; несанкционированный доступ (НСД) к корпоративной информации; информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб; действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации; техногенные катастрофы.

Для компании по организации мероприятий стоят задачи по сбору информации о своих клиентах, их контактов, личных предпочтений, месте и времени проведения мероприятия. После проведения мероприятия на носителях информации хранятся фотографии, видеоклипы с участием всех гостей мероприятия. Секретность и конфиденциальность информации наиболее уязвимы, когда такая информация транспортируется через общедоступную сеть Интернет, поэтому при передаче информации через Интернет ожидает­ся, но не гарантируется секретность. Также event-компания должна хранить информацию о контактах компаний-сотрудников, например, аренды площадок для мероприятий, аренды транспорта и т.д. Таким образом, можно сказать, что утечка информации может стоить event-компании потери репутации как в лице клиентов, так и компаний-партнёров.

# Оценка угроз, рисков и уязвимостей

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб агентству |
| 1 | Ущерб от атаки есть, но он незначительный, основные финансовые операции и положение агентства на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время агентство терпит убытки, но его положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От агентства уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, агентство на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |
| 5 | Агентство прекращает существование |

|  |  |
| --- | --- |
| 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 |

**Оценка рисков**

|  |  |  |  |
| --- | --- | --- | --- |
| Описание Атаки | Ущерб | Вероятность | Риск |
| разглашение информации сотрудниками агентства | 4 | 0,2 | 0,8 |
| кибератака | 4 | 0,2 | 0,8 |
| подслушивание конфиденциальных разговоров | 2 | 0,3 | 0,6 |
| утеря носителей информации | 1 | 0,2 | 0,2 |
| спам | 1 | 0,3 | 0,3 |
| копирование информации из отдела бухгалтерии | 2 | 0.1 | 0,2 |
| копирование жесткого диска из главного офиса | 4 | 0,1 | 0,4 |
| недостаточная квалификация персонала | 2 | 0,3 | 0,6 |
| природные явления | 2 | 0,3 | 0,6 |
| Итого |  |  | 4,5 |

# Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.

Первым шагом является обучение основным принципам компьютерной безопасности гостей и участников мероприятия. Они должны быть осведомлены о рисках, связанных с их данными, а организаторы мероприятий должны убедиться, что они предлагают простые и понятные действия для сохранения целостности данных.

Второй шаг касается защиты самих данных. Необходимо создать компьютерный щит, который будет противостоять потенциальным атакам и гарантировать, что компьютеры и другие подключенные устройства защищены техническими решениями, такими как антивирусное программное обеспечение, зашифрованные данные и безопасные соединения.

Третий шаг - убедиться, что среда, в которой расположены устройства, безопасна. Решения варьируются в зависимости от уровня риска - от неразглашения информации об используемых помещениях до обнаружения и блокировки шпионского оборудования, микрошпионов, мини-камер или других систем прослушивания и сбора информации.

Необходимо убедиться, что на месте проведения мероприятия установлены соответствующие камеры видеонаблюдения, чтобы удерживать людей от кражи личного имущества.

Также стоит убедиться, что нанято достаточно сотрудников службы безопасности для наблюдения за мероприятием. Если используется дорогое оборудование, убедитесь, что к нему имеет доступ лишь ограниченное количество людей. Сотрудники службы безопасности должны немедленно сообщать о подозрительных людях на мероприятии.

Требования, предъявляемые к надежности системы и ее информационной безопасности:

* исключение возможности просмотра, изменения или уничтожения информации лицами, не имеющими на это права;
* исключение несанкционированного доступа к информации, для обеспечения предотвращения утечки обрабатываемой информации;
* предотвращение различного рода воздействий, которые способны вызвать изменение, уничтожение и искажение информации, а также сбои в работе средств автоматизации;
* предотвращение утечки информации за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники;
* подотчетность (руководитель должен всегда знать, кто работает в системе и с чем).

*Программное обеспечение*

Выбранное программное обеспечение и технические средства обеспечивают целостность баз данных при любых нарушениях в системе безопасности.

На компьютерах агентства должна использоваться шифрованная файловая система — система шифрования данных, реализующая шифрование на уровне файлов в операционных системах. Данная система предоставляет возможность «прозрачного шифрования» данных, хранящихся на разделах с файловой системой, для защиты потенциально конфиденциальных данных от несанкционированного доступа при физическом доступе к компьютеру и дискам

Также для защиты компьютеров используются антивирусные программы. Они предназначены для:

* антивирусной проверки файлов, программ и веб-сайтов
* анти-фишинга
* контроля интернет-трафика
* защиты от программ-шифровальщиков
* поиска уязвимостей

*Организационно-административные методы* защиты информации — это меры, регламентирующие процессы функционирования системы, использование ее ресурсов, деятельности персонала, а также порядок взаимодействия пользователей системой таким образом, чтобы максимально затруднить или исключить возможность реализации угроз безопасности информации. А именно:

* наличие надлежащей настройки операционных систем и программного обеспечения сервера, рабочих мест пользователей;
* выделение специальных ЭВМ для обработки конфиденциальной информации;
* наличие межсетевого программно-аппаратного экрана (firewall, брандмауэр, МСЭ), контролирующего доступ к сети;
* наличие специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;
* организация регламентированного доступа пользователей к работе на ЭВМ, средствах связи и в хранилищах носителей конфиденциальной информации;
* установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;
* создание и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации;
* постоянный контроль за соблюдением установленных требований по защите информации.

*Организационно-техническая защита информации:*

* отключение ЭВМ от локальной вычислительной сети или сети удаленною доступа (региональные и глобальные вычислительные сети) при обработке на ней конфиденциальной информации, кроме случаев передачи этой информации по каналам связи;
* организация электропитания ЭВМ от отдельного блока питания;
* использование бесперебойных источников питания для персональных компьютеров для силовых электрических сетей с неустойчивым напряжением и плавающей частотой.

*Физические меры защиты* — различные механические, электро- или электронно-механические устройства, предназначение для создания физических препятствий на путях проникновения потенциальных нарушителей к защищаемой информации, а также техник визуального наблюдения, связи и охранной сигнализации. А именно:

* перекрытие незаконным пользователям физического доступа к месту, где имеется (хранится или передается) защищаемая информация;
* установки аппаратуры компьютерной системы, что называется, под замком в помещении, снабженном сигнализацией, надежной охраной аппаратных и узлов управления, электромагнитным экранированием зданий и помещений, камерами видеонаблюдения;
* установка специальных сейфов и металлических шкафов для установки в них отдельных узлов и блоков компьютера для вычислительной системы (принтер, файл-сервер).

*Технические (аппаратно-программные) средства защиты*— различные электронные устройства и специальные программы, выполняющие (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию пользователей, разграничение доступа к ресурсам, криптографическое закрытие информации).

* аутентификация партнеров по взаимодействию, позволяющая убедиться в подлинности партнера при установлении соединения;
* аутентификация источника информации, позволяющая убедиться в подлинности источника сообщения;
* управление доступом, обеспечивающее защиту от несанкционированного использования ресурсов;
* конфиденциальность данных, которая обеспечивает защиту от несанкционированного получения информации;
* целостность данных, позволяющая обнаружить, а в некоторых случаях и предотвратить изменение информации при ее хранении и передаче;
* принадлежность, которая обеспечивает доказательство принадлежности информации определенному лицу.

# Вывод

При разработке политики информационной безопасности любой организации важно следовать четкой последовательности. Оценив структуру организации, необходимо выявить её слабые места, проанализировать возможные виды атак и рисков. После оценки рисков необходимо выделить из них наиболее вероятные и разработать систему мер защиты о них. Любая организация имеет свои индивидуальные особенности по работе с информацией и это стоит учитывать при разработке мер по защите информации.

Для компании, занимающейся организацией мероприятий, важно разработать систему, по которой каждый сотрудник будет осведомлён о надлежащих мерах защиты своего рабочего места, рабочего аккаунта и будет иметь доступ только к той информации, с которой ему необходимо работать. Важно регулярно проводить осмотр техники и надлежащую замену оборудования, чтобы избежать потери как личных данных клиента, так и материала с мероприятий, а также соблюдать меры пожарной безопасности во избежание стихийных бедствий, которые повлекут за собой не только потерю данных клиентов, но и порчу оборудования, и, конечно, репутацию самой компании.

Все эти меры гарантируют, что информация, передаваемая в пространстве событий, не будет захвачена, а такие устройства, как мобильные телефоны, планшеты или компьютеры, не могут быть сканированы удаленно.