МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа № 1**

**РАЗРАБОТКА И ВНЕДРЕНИЕ**

**ПОЛИТИКИ БЕЗОПАСНОСТИ**

для event-компании

Разработал: Бай И.О.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

# **Введение**

В XXI веке информационные технологии нужны всем компаниям, чтобы быть конкурентоспособными в условиях широкого использования высокотехнологичных решений. Информационные ресурсы в современном обществе являются наиболее важными, но в то же время очень уязвимыми. механизм их распространения становится все более гибким и увеличивается число путей их передачи. В связи с этим информационная безопасность является одним из важнейших условий функционирования любой структуры.

Жизнь современного общества немыслима без информационных технологий. Программные средства управляют банковскими системами, распределяют энергию, следят за расписанием поездов. Они обеспечивают хранение информации, ее обработку и предоставление потребителям и тем самым реализуют информационные технологии.

Темпы развития современных информационных технологий значительно опережают темпы развития рекомендательно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение задачи разработки эффективной политики информационной безопасности на современном предприятии неизбежно связано с проблемой выбора критериев и показателей безопасности.

Высокая степень автоматизации таит в себе риск снижения личной, информационной и государственной безопасности и делает ее чрезвычайно уязвимой. Поэтому, помимо требований и рекомендаций стандартов, Конституции, законов и других соответствующих документов, мы должны ссылаться на ряд международных рекомендаций. Это включает в себя адаптацию к национальным условиям и внедрение методов международных стандартов, а также использование методов управления информационными рисками в сочетании с оценками экономики инвестиций для обеспечения защиты корпоративной информации.

**Обоснование актуальности**

Каждой компании, ведущей свой бизнес, приходится работать с информацией везде и всегда, как при планировании долгосрочных стратегических задач, так и в повседневной офисной жизни. С бурным развитием науки и техники появилось множество методов и средств работы с информацией, иногда настолько сложных, что их применение, их адаптация к специфике конкретного предприятия и условиям, в которых оно сегодня находится, составляют уже отдельный класс задач.

**Цель информационной безопасности event-компании:** обеспечение защиты информации, предоставление конфиденциальности клиентам.

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 государства 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;
* регламенты обращения с компьютерной техникой и средствами коммуникации;
* реализация осведомления сотрудников о возможных рисках угроз ИБ и обучение мерам противодействия.

Безопасность мероприятия – основа качественного оказания ивент услуги. Почему важно не экономить на этой статье расходов? Организация мероприятия – это предпринимательская деятельность, направленная в числе прочего на получение прибыли. Экономия бюджета непосредственным образом влияет на безопасность, что может привести к тяжким последствиям в виде причинения вреда здоровью, а иногда и наступления смерти участников мероприятия.

Однако оказывать услуги предоставления безопасности нужно не только во время проведения самого мероприятия, а задолго до этого. Разработка гибкой и отлаженной структуры ИБ поможет компании избежать таких проблем, как незаконный перекуп билетов, утечка конфиденциальной информации пользователей, организаторов мероприятий и даже других компаний, которые тем или иным способом были задействованы в организации и проведении мероприятия.

**Объекты защиты**

Структура event-компаний чаще всего выглядит таким образом:

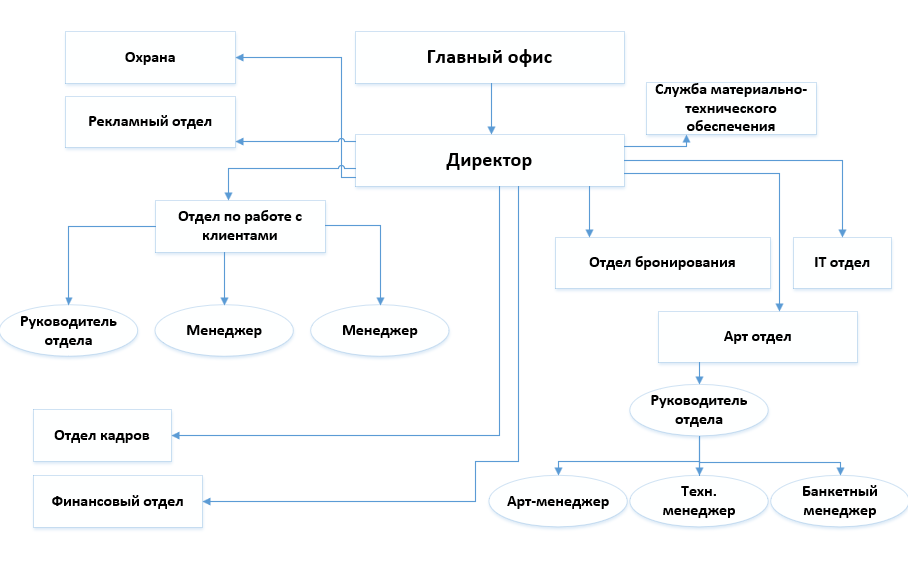


Рисунок 1 – Структура event-компании

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

К объектам защиты event-компании относят:

* коммерческая тайна самой event-компании, данные о ее договорах, финансовых взаимоотношениях, бухгалтерская информация;
* конфиденциальность клиентов и партнеров организации;
* персональные данные сотрудников компании, эта информация иногда включает номера телефонов, кредитных карт, домашние адреса;
* места проведения мероприятий.

В качестве субъектов информационных отношений чаще всего выступают клиенты, сотрудники, партнеры компании, а также такие электронные устройства как компьютер, телефон, планшет и др.

**Основные угрозы и их источники**

В зависимости от критерия классификации, угрозы информационной безопасности event-компании 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:

* землетрясение;
* наводнение;
* пожары.

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

* халатное обращение сотрудников с техникой;
* повреждение техники;
* угроза использования не лицензионных программ.

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

* использование работниками компьютеров в своих целях;
* невнимательность сотрудников;
* установка вредоносных программ;
* предоставление ошибочных данных клиентами.

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

* + троян;
  + rootkit;
  + IP спуфинг;
  + фишинг;
  + спам;
  + установка вредоносного ПО;
  + фальсификация данных;
  + кража конфиденциальных данных;
  + саботаж.

*Источники угроз* безопасности информации event-компании:

* нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов event-компании, а также фальсификация (подделка) документов;
* разглашение, передача или утрата конфиденциальных данных (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
* перехват данных, передаваемых по каналам связи, и их анализ.

**Оценка угроз, рисков и уязвимостей**

Согласно статистике, все event-компании 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 event-компании зачастую приводит к вымогательству и шантажу, инсайдерской торговле и недобросовестной конкуренции. Это не только нанесет урон репутации – фирма 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 event-компании

|  |  |
| --- | --- |
| 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 event-компании. 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 |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | 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** |
| Нападения, кражи и проникновения | 4 | 0,1 | 0,4 |
| Кража конфиденциальных данных | 3 | 0,4 | 1,2 |
| Трояны | 2 | 0,5 | 1 |
| Rootkit | 2 | 0,5 | 1 |
| Невнимательность сотрудников | 3 | 0,2 | 0,6 |
| IP спуфинг  (получ. IP относящегося к компании) | 2 | 0,3 | 0,6 |
| Фишинг | 2 | 0,3 | 0,6 |
| Пожар, сбой в подаче электроэнергии | 4 | 0,2 | 0,8 |
| Повреждение техники | 3 | 0,4 | 1,2 |
| Невнимательность сотрудников по отношению к данным клиентов | 2 | 0,5 | 1 |
| Невнимательность сотрудников к техническому оборудованию | 3 | 0,5 | 1,5 |
| Предоставление клиентами ошибочных данных | 1 | 0,5 | 0,5 |
| Природные катаклизмы | 5 | 0,1 | 0,5 |
| Установка вредоносного ПО | 3 | 0,4 | 1,2 |
| Фальсификация данных | 3 | 0,3 | 0,9 |
| Саботаж и клевета | 3 | 0,2 | 0,6 |
| **Итого** |  |  | 13,6 |

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

**Разработка мер защиты**

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

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

* + Наличие охраны
  + Наличие пропускной системы для рабочего персонала
  + Наличие IT специалиста по кибер-безопасности
  + Установка только официального ПО
  + Запрет сотрудникам установки других программ
  + Передача адреса электронной почты только проверенным источникам
  + Использование только проверенных ресурсов и путей доступов к ним
  + Шифрование данных
  + Использование новейших средств защиты
  + Приём на работу квалифицированных сотрудников
  + Использование Брандмауэра сети
  + Связь офиса с МЧС, милицией и пожарной службой
  + Инструктаж персонала
  + Проведение регулярных бесед и инструктажей с сотрудниками

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

**Вывод**

В ходе выполнения лабораторной работы были выявлены все возможные угрозы и их источники информационной безопасности в event-компании, а также проанализированы и оценены собранные данные.

На основании этого была разработана концепция и основные элементы политики безопасности для event-компании.

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.