МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №1**

по дисциплине «Криптографические методы защиты информации»

на тему: РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ИЛИ УЧРЕЖДЕНИЯ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

Содержание

[1. Обоснование актуальности, цели и задачи разработки ПИБ в организации (учреждении) 3](#_Toc127169415)

[2. Объекты защиты 4](#_Toc127169416)

[3. Основные угрозы и их источники 5](#_Toc127169417)

[4. Оценка угроз, рисков и уязвимостей 7](#_Toc127169418)

[5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов 9](#_Toc127169419)

[Выводы 10](#_Toc127169420)

# 1. Обоснование актуальности, цели и задачи разработки ПИБ в организации (учреждении)

***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.

**Актуальность ПИБ** состоит в том, чтобы не допустить законодательно или на основе правил утечки конфиденциальной информации event-компаний в свободный доступ.

**Цели:**

* Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* Соблюдение конфиденциальности информации ограниченного доступа;
* Реализацию права на доступ к информации.

**Задачи:**

* Установка объектов защиты;
* Установка основных угроз и их источников;
* Оценка угроз, рисков и уязвимостей;
* Установка мер, методов и средств обеспечения требуемого уровня защищенности информационных ресурсов.

# 2. Объекты защиты

Event Management Company или как вы можете встретить ивент-агентство – это компания, которая занимается организацией разного рода мероприятий сферы развлечений (корпоративы, праздники и т.д.).

В широком смысле все события могут быть классифицированы как:

* MICE — Meetings, Incentives, Conferences and Exhibitions (встречи, инициативы, конференции и выставки);
* Сферы искусств, такие как: пьесы, музыкальные спектакли, танцевальные выступления и т.д.;
* Сфера отдыха и образа жизни — события начиная от спорта и отдыха, мода, тематические мероприятия, связанные с социальными, и общественными события.

Структура расположения event-компаний – это офисы. Небольшие помещение способствуют меньшему риску со стороны количества персонала, но в то же самое время — это центральное место расположения компании. В основном компании арендуют офисы в специальных местах, где раздают помещения под офисные или рабочие пространства, соответственно существует угроза со стороны конкурентов и воровства коммерческой тайны.

Структура event-компаний:

* Генеральный директор;
* Отдел развития (new business) — отвечает за поиск и привлечение новых Клиентов, участие в тендерах заказчиков.
* Отдел по работе с Клиентами — группа менеджеров, которые являются связующим звеном между Клиентом и event-компанией.
* Творческий (креативный) отдел — отвечает за создание концепций мероприятия и другого креатива. Здесь работают копирайтеры (отвечают за текстовую часть рекламы), режиссеры, сценаристы. Отдел возглавляет один или несколько креативных директоров.
* Производственный отдел — дизайнеры, специалисты по производству (продакшн). Люди, помогающие воплотить идею, рожденную в креативном отделе. Менеджеры этого отдела заказывают услуги подрядчиков event-компании.
* Финансовый отдел — подразделение, выполняющее ряд важных функций финансового контроля для полноценного функционирования всей структуры;
* IT-отдел: поддержка внешних и внутренних серверов компании, системное администрирование, поддержка пользователей;
* Менеджер по персоналу: осуществляет весь цикл работ с персоналом: от изучения рынка труда и найма персонала до ухода на пенсию и увольнения.

Угроза выведения из строя компьютеров конкурентами или получение доступа к базам данных. Доступ к офису имеют: начальство, сотрудники, арендодатели и уборщики помещений (опционально).

***Объект*** – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию.

**Объекты защиты**: сетевые каналы передачи информации, помещение, договора.

***Субъект*** – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

**Субъекты защиты**: сотрудники, заказчики, аппаратные средства (компьютер), программные средства.

# 3. Основные угрозы и их источники

Все многообразие потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: *естественные* (объективные) и *искусственные* (субъективные).

***Естественные угрозы*** – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

***Искусственные угрозы*** – это угрозы, вызванные деятельностью человека.

***Непреднамеренные*** (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей ИВС (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов ИВС.

***Преднамеренные*** (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т. п.) действия легально допущенных к информационным ресурсам пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы.

Естественные угрозы:

* Пожары;
* Ураганы;
* Наводнения.

Искусственные угрозы:

* Непреднамеренные угрозы:
  + Производственный брак аппаратных средств;
  + Ошибки пользователей и обслуживающего персонала;
  + Разговоры на тему работы.
* Преднамеренные угрозы:
  + Атаки на сервер;
  + Вредительские программы;
  + Несанкционированный доступ к информации, в том числе персональной;
  + Перехват данных;
  + Кража документов;
  + Восстановление удаленной информации с жестких дисков;
  + Обвал сайта;
  + Дезинформация;
  + Подкуп и шантаж сотрудников;
  + Наблюдение;
  + Подслушивание;
  + Проникновение в помещение и вредоносные действия посторонних лиц;
  + Рассылка на почту.

Источники угроз по отношению к самой информационной системе могут быть как *внешними*, так и *внутренними*.

Внешние угрозы:

* Атаки со стороны конкурентов;
* Атака со стороны мошенников.

Внутренние угрозы:

* Атаки со стороны сотрудников.

# 4. Оценка угроз, рисков и уязвимостей

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ.

Условная численная шкала для оценки ущерба компании

|  |  |
| --- | --- |
| **Величина ущерба** | **Описание** |
| 0 | Раскрытие информации, не являющейся конфиденциальной и не раскрывающая данных о заказчиках |
| 1 | Ущерб атаки есть, но он незначителен и не связан с положением компании на рынке |
| 2 | Существует вероятность потери некоторого числа клиентов, компания теряет часть прибыли |
| 3 | Потеря весомой доли клиентов и потеря доли рынка, компания несет убытки |
| 4 | Полная потеря рынка и конкурентоспособности, долги, а так же полная потеря клиентов, банкротство |
| 5 | Полное банкротство компании и прекращение существования |

Вероятность того, что угроза реализуется, определяется на основе следующих факторов:

* Привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* Возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* Технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
* Вероятность того, что угроза реализуется;
* Степень легкости, с которой уязвимость может быть использована.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

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 проверяется каждая строка таблицы: превышен или не превышен порог для значения риска, связанного с анализируемой атакой? Если такое превышение имеет место, данная атака должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности.

Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки** | **Ущерб** | **Вероятность** | **Риск** |
| Несанкционированный доступ к информации | 3 | 0,3 | 0,9 |
| Разговоры на тему работы | 2 | 0,2 | 0,4 |
| Подкуп и шантаж сотрудников | 2 | 0,2 | 0,4 |
| Наблюдение, подслушивание | 2 | 0,1 | 0,2 |
| Рассылка на почту | 2 | 0,2 | 0,4 |
| Проникновение в помещение и вредоносные действия посторонних лиц | 3 | 0,1 | 0,3 |
| Сбои и отказы технических средств | 3 | 0,1 | 0,3 |
| Перехват данных | 3 | 0,1 | 0,3 |
| Кража информации | 3 | 0,2 | 0,6 |
| Компьютерные вирусы | 3 | 0,1 | 0,3 |
| Восстановление | 3 | 0,1 | 0,3 |
| Обвал сайта | 1 | 0,1 | 0,1 |
| Дезинформация | 3 | 0,1 | 0,3 |
| Стихийные бедствия | 2 | 0,1 | 0,2 |
| Итого |  | | 5,0 |

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

После того как документация по информационной безопасности готова, необходима плановая деятельность по ее внедрению в повседневную работу. Основу таких мероприятий, как было указано в плане выполнения лабораторной работы, составляют инструкции, содержащие подробное описание (алгоритмы) действий по организации информационной защиты и обеспечению разработанных стандартов и процедур, и план мероприятий по обучению персонала и тестированию знаний сотрудников, имеющих доступ к информационным ресурсам.

Можно выделить следующие общие направления мероприятий:

* Управление персоналом;
* Физическая защита инфраструктуры ИВС;
* Поддержание работоспособности ИВС;
* Реагирование на нарушения режима безопасности ИВС;
* Планирование восстановительных работ.

Методы обеспечения требуемого уровня защищенности информационных ресурсов:

* Установление норм и правил в договорах сотрудников о коммерческой тайне;
* Ограничение сторонних лиц внутри офиса (Установление камер видеонаблюдения и систем карточных пропусков);
* Установка паролей и соответствующего ПО;
* Установка градации сотрудников и их уровней доступа к информации;
* Информирование или переобучение персонала;
* Обеспечение технической защиты помещений и оборудования, определение их соответствия нормативно-правовым требованиям;
* Выполнение всех требований законодательства по защите персональных данных;
* Использование средств антивирусной защиты;
* Использование менеджера паролей;
* Защита, разграничение сервисов;
* Отказ от нешифрованного трафика (Использование HTTPS вместо HTTP);
* Использование сертифицированных аппаратных средств;
* Использование средств криптографической защиты.

# Выводы

Event-компания обладает относительно низким риском потери информации в любом из его проявлений, однако политика безопасности представленная выше при соблюдении всеми сотрудниками компании поможет снизить риск потери информации до минимума.