**Задание 1. Заполнение технологической карты ОТС**

**(опасных техногенных событий)**

**Технологическая карта**

|  |  |  |  |
| --- | --- | --- | --- |
| **Вид** | **Информационная / экономическая / экологическая безопасность** | | |
| **Виды опасностей, наиболее распространенные в настоящее время** | Хищение информации, информационная и игровая зависимость, воздействие информационной среды (в том числе избыточность информации), опасности в сети Интернет. | | |
| **Действующее законодательство в области заданного направления безопасности** | * Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; * Статья 29 — право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации; * Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 — право на знание достоверной информации о состоянии окружающей среды. | | |
| **Примеры** | * **Троянские программы** (программы, которые выполняют несанкционированные пользователем действия на поражаемых компьютерах. Например, уничтожают информацию на дисках, приводят систему к зависанию, воруют конфиденциальную информацию и тому подобное); * **Программы-майнеры;** * **Программы-шпионы;** * Взлом учетной записи, личных аккаунтов в соц.сетях. | | |
| **Виды опасностей, источники** | **Причины возникновения** | **Возможные последствия** | **Действия по профилактике / предупреждению** |
| ***Угрозы целостности*** | * Ошибка оператора может привести к тому, что данные перестанут отражать реально-существующие отношения в предметной области. * К нарушению целостности могут привести и внутренние отказы ИС, и любые внешние случайны или намеренные воздействия. * Нарушение целостности может привести и к нарушению доступа к данным. Если в информационном хранилище содержится информация о платежах, которые произвело предприятия, а номер месяца, в котором произведен данный платеж, окажется большим 12, то следствие может быть каким угодно, начиная от выдачи неверных данных и заканчивая сбоем в работе всей системы. Все зависит от того, какие алгоритмы обработки данных используются в информационной системе. | Нарушение целостности информации | * Транзакционные механизмы, позволяющие восстановить целостность данных в случае незначительных сбоев. * Контроль ввода данных. Много ошибок можно было бы избежать, если программы не пропускала бы заведомо противоречивые данные. * Использование средств защиты целостности СУБД. * Резервное копирование данных. * Периодическое тестирование системы на предмет нарушения целостности. |
| ***Угроза доступности*** | * отказ пользователей; * внутренний отказ информационной системы; * отказ поддерживающей инфраструктуры. | Нарушение доступа к информации, к базе данных. | * Правильная организация труда. Многие проблемы возникают благодаря не совсем продуманному распределению обязанностей; * Подготовка и подбор кадров, в том числе и системных администраторов, в задачу которых будет входить конфигурирование системы; * Тщательная и полная разработка информационной системы, в том числе удовлетворяющего работников пользовательского интерфейса; * Тщательное тестирование информационной системы, в том числе и на предмет критических ситуаций (при большой нагрузке, больших объемах обрабатываемой информации и т.п.), и на предмет ввода заведомо неправильной информации; * Резервное копирование данных, позволяющее в любой момент восстановить поврежденные данные с минимальными потерями. Под резервным копированием следует понимать не только непосредственное создание резервных копий, но и такие механизмы как зеркалирование и кластеризация (объединение нескольких СУБД в кластеры); * Наличие резервного оборудования, помещений, подготовка персонала к действию на случай нештатных ситуаций; * Средства защиты каналов связи, например от воздействия внешнего электромагнитного излучения. |
| ***Угроза конфиденциальности*** | * отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа; * неэффективную систему защиты информации или отсутствие этой системы, что образует высокую степень уязвимости информации; * непрофессионально организованную технологию обработки и хранения конфиденциальных документов; * неупорядоченный подбор персонала и текучесть кадров, сложный * психологический климат в коллективе. | Утечка данных, попадание информации в руки посторонних людей. | Во-первых, проводите регулярные аудиторские проверки безопасности всех представительств на соблюдение договорных и государственных обязательств наряду с другими областями бизнеса, включая дата-центры. Мы проводим аудит каждый год, чтобы у нас было независимое мнение об операционных процессах компании.  Во-вторых, внедрите единую систему корпоративных правил, которые обязывают сотрудников соблюдать чистоту рабочего стола и запрещают использовать на рабочем месте любые устройства, которые могут хранить и передавать данные. Эти правила охватывают все: от входа в систему до пропускного режима и обустройства рабочего пространства. Они должны определять границы того, что можно и нельзя делать в компании. Менеджер по информационной безопасности должен контролировать их выполнение.  В-третьих, мы создали и внедрили систему, которая позволяет менеджерам обнаружить уязвимость на ранних этапах. Она должна включать защиту от мошенничества и инструменты, которые мониторят подозрительную активность и сообщают о ней. Сотрудники должны проходить тренинги в соответствии с их уровнем доступа и рабочими обязанностями.  В-четвертых, обучайте правилам информационной безопасности сотрудников всех уровней – от начинающих специалистов до топ-менеджмента. Создайте горячую линию, мотивируйте сотрудников к открытой коммуникации и немедленном информировании о подозрительной активности. Наш подход объединяет нормы, безопасность и конфиденциальность данных как единое целое, контролируемое топ-менеджментом. Это позволяет нам быстро реагировать на любые потенциальные угрозы.  В-пятых, система безопасности должна быть контролируема и задокументирована. Мы используем данные с аудиторских проверок и накопленные опыт, а также собираем информацию от нашей операционной команды, чтобы улучшать процессы и разрабатывать более эффективные инструменты. Кроме того, мы изучаем опыт наших коллег на глобальном рынке с точки зрения безопасности, а также делимся экспертизой с клиентами и профессиональным сообществом. |