Работа с ГОСТами в области информационной безопасности

Цель работы на основе ГОСТ Р 53114-2008 получить навыки составления документации в области информационной безопасности.

Практическое задание

1. На основе ГОСТ Р 53114-2008 составить памятку об информационной безопасности для заведения, использующего электронный документооборот

ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОЙ ДОКУМЕНТАЦИИ НЕОБХОДИМО:

* Использование политики конфиденциальности;
* Использование проверенного программного обеспечения и сертифицированных антивирусных программ;
* Профилактика несанкционированного доступа к частной информации;
* Использование закрытых сетевых серверов во избежание блокировки доступа к информации лиц, имеющих на это право;
* Чтобы не допустить утечку информации необходимо навсегда удалять со всех информационных носителей информацию, которая уже не используется, а также тщательно контролировать сохранение информации на внешних носителях;
* Ограничение доступа в интернет для сотрудников поможет избежать перехвата информации;
* Использование локальных серверов для профилактики электромагнитных излучений;
* Перенаправление сотрудника, столкнувшегося с проблемами на компьютере компании, в центр информационной безопасности компании;
* Проводить слежку для сотрудника чтобы избежать утечки информации.

2. Обосновать достаточность предлагаемых пунктов безопасности.

Я написал данную памятку на основе документа ГОСТ Р 53114-2008 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ», здесь подробно описаны проблемы, с которыми может столкнуться компания в сфере информационной безопасности. Так же здесь описаны угрозы. Я просмотрел весь документ и исходя из содержания значений и терминов сделал выводы о том, как необходимо защищать информацию в организации использующей электронный документооборот.

3. На примере продемонстрировать необходимость соблюдения правил информационной безопасности.

В компании Microsoft, в 2004 году украли исходный код Windows 2000 и Windows NT. Эта информация является самой ценной информации для Операционной системы, с помощью украденного кода злоумышленники могли написать вредоносную программу, которая бы обходила антивирусы. Эти данные были выложены в глобальную сеть интернет и стремительно разлетелись по всему миру. Сначала все думали, что кражу совершил один из партнеров Microsoft, но затем выяснилось, что это был один из сотрудников компании. Вскоре компания отказалась от ОС Windows 2000 и Windows NT. Ущерб был не большим, но эта ситуация нанесла большой урон по репутации компании.

Данный пример доказывает, что для сохранения конфиденциальной информации компании необходимо использовать правила информационной безопасности, а конкретно такие как «Осуществление слежки за сотрудниками компании» и «Ограничение доступа в интернет для сотрудников».

Контрольные вопросы

1. Какие стандарты включены в ГОСТ Р 53114-2008?

* Безопасность в чрезвычайных ситуациях;
* Система менеджмента качества;
* Системы экологического менеджмента;
* Информационные технологии. Методы и Средства обеспечения безопасности. Часть 1 и Часть 2;
* Защита информации. Основные термины и понятия;
* Защита информации. Объект информатизации. Факторы, воздействующие на информацию;
* Менеджмент риска.

2. Что такое приемлемость уровня риска?

Определение приемлемости уровня риска – это процесс сравнения результатов анализа риска с критериями риска с целью определения приемлемости или допустимого уровня риска.

Выводы: Я изучил положение ГОСТ Р 53114-2008 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ». Составил памятку для компании, использующей электронный документооборот и доказал, как важно использовать правила информационной безопасности на примере кражи информации у Microsoft.