Отчёт выполнила Шпанагель Дарья

Студент группы БИСО-03-19

**Практика №1 по дисциплине**

**«Основы информационной безопасности»**

**«Политика безопасности»**

Задание :

Составить политику информационной безопасности для собственной организации. Составить технический регламент, инструкцию для одного из отделов.

Решение :

Пусть существует компания ООО «Старт».

Штат — 77 сотрудников:

* 3 — руководство ;
* 6 — бухгалтерия ;
* 8 — IT-отдел ;
* 50 — менеджеры по работе с клиентами ;
* 10 — отдел безопасности.

Управление компании использует телефонную связь, MS Office, 1С:Предприятие и т. д.

Бухгалтерия использует телефонную связь, MS Office, 1С:Бухгалтерию.

IT-отдел обеспечивает функционирование внутренней сети организации, а также сайта компании и личных кабинетов клиентов.

Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет. Телефонной связи и др.

Отдел безопасности схож с IT-отделом, но также имеет доступ к проведению тестирований системы на наличие уязвимостей.

Технический же регламент для отдела информационной безопасности выглядит так :

* Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
* Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
* Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
* Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
* Учет машинных носителей персональных данных;
* Обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
* Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
* Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
* Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.