Компания ООО «Umbrella». Управление компании использует телефонную связь и защищенное интернет соединение. Бухгалтерия использует телефонную связь и защищенное интернет соединение.

Штат – 100 сотрудников.

10 – руководство.

10 – отдел безопасности.

25 – ученые.

5 – бухгалтерия.

50 – вооруженная охрана.

Руководство получает уведомление по поводу проведения секретных экспериментов в лаборатории, используя телефонную связь (передача шифрованной речи осуществляется по каналам CSD 9600 бит/с) и уведомление о передаче этапов работы на компьютер. Передача этапов работы происходит через защищенное интернет соединение. Вся документация защищена паролем. Имеет полный доступ ко всем помещениям организации.

Отдел безопасности занимается организацией и обеспечением защиты любой информации, полученной на территории организации. Обеспечивают руководство физическим вводом ключа при получении. Использует любую связь, исключительно скрытую. Имеет доступ к местам хранения информации организации.

Ученые получают указания от руководства по проведению экспериментов. Результаты сохраняются на сервер организации. Имеют доступ к помещениям для проведения экспериментов.

Бухгалтерия занимается учетом финансов и подтверждением документов на те или иные ресурсы, требующиеся для экспериментов. Используют телефонную связь. Имеет доступ к помещению бухгалтерии.

Вооруженная охрана находится на территории всей организации. На выходе из организации установлен пункт досмотра. Каждый входящий и выходящий из организации обязан пройти досмотр на присутствие запрещенных предметов. Имеет доступ к местам перемещения по организации, могут запросить доступ к другим помещениям по необходимости.

Технический регламент для отдела безопасности:

-Постоянный анализ информационного пространства с целью выявления уязвимостей.

-Своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность, корректировка моделей угроз и нарушителя.

-Исключать возможность доступа третьих лиц к документам, содержащим конфиденциальную информацию.

-Контролировать состояние рабочего места, сообщать руководству обо всех ситуациях, имеющих характер инцидентов информационной безопасности.

-Регулярно выявлять основные пути и способы попадания зараженной вирусом информации в систему организации.

Инструкция для специалиста по безопасности:

Специалист должен знать:

-Основы трудового законодательства.

-Законодательство о безопасности, о защите информации, об оперативно-розыскной деятельности и др.

-Устав организации, правила внутреннего порядка.

-Характеристики технических средств защиты объектов, информации от несанкционированного доступа к ним.

-Тактику защиты объектов, информации, персонала предприятия от преступных посягательств.

-Характеристику технических средств (системы сигнализации, связи, защиты информации, пр.).