1. Охарактеризовать актуальность и основные причины про блемы информационной безопасности организации, страны.
2. Сформулировать цели и задачи политики информационной безопасности.
3. Охарактеризовать основные угрозы информационной безо пасности каждой организации (учреждения) из табл. 1.4.
4. Как правильно проводить оценку рисков?
5. Что должна включать в себя программа внедрения полити ки информационной безопасности?

1.**Актуальность и основные причины проблемы информационной безопасности**

-

Р

ост

объема

и

значимости

цифровой

информации.

-

У

величение

числа

кибератак

и

утечек

данных.

-

Р

азвитие

технологий,

требующих

надежной

защиты

данных.

-

З

аконодательные

требования

к

защите

информации.

-

В

озможность

значительных

финансовых

и

репутационных

потерь.

1. **Цели и задачи политики информационной безопасности**

Защита конфиденциальности, целостности и доступности данных.

Обеспечение надежности информационных систем.

Управление рисками и угрозами безопасности.

Разработка и внедрение мер защиты информации.

Повышение осведомленности персонала о правилах ИБ.

1. **Основные угрозы информационной безопасности организаций**

**Учебные заведения (школа, университет, библиотека)** – утечка персональных данных студентов и преподавателей, несанкционированный доступ к учебным материалам.

**Банки, страховые, юридические компании** – кража финансовых данных, мошенничество.

**Поликлиники, больницы** – утечка медицинских данных.

**ИТ-компании, мобильные операторы** – атаки на инфраструктуру, взлом клиентских данных.

**Издательства, маркетинговые компании** – кража интеллектуальной собственности.

**Логистические, туристические компании** – компрометация персональных и финансовых данных клиентов.

**Как правильно проводить оценку рисков?**

Идентифицировать активы, подлежащие защите.

Определить потенциальные угрозы и уязвимости.

Оценить вероятность реализации угроз.

Рассчитать возможный ущерб.

Разработать меры по снижению рисков.

**Что должна включать в себя программа внедрения политики информационной безопасности?**

Определение ответственных лиц и ролей в системе безопасности.

Разработка нормативных документов (правил, инструкций, регламентов).

Технические меры защиты (антивирусы, брандмауэры, контроль доступа).

Организационные меры (обучение персонала, аудит безопасности).

План реагирования на инциденты и аварийные ситуации.

***Политика информационной безопасности* (*ПИБ*)** – совокупность правил, процедур, методов, направленных на защиту информации и связанных с ней ресурсов.

***Информационная (ИВ) система***– упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы.

***Информационные процессы***– процессы сбора, накопления, хранения, обработки (переработки), передачи и использования информации.

***Информационные ресурсы***– отдельные документы в ИС.

***Объект*** *–* пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

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

***Доступ*** *–* спец тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

***Атака***– попытка несанкционированного преодоления защиты системы.

***Несанкционированный доступ (НСД)***– доступ к информации, реализуемый без ведома (санкции) владельца.

***Защита информации***– организационные, правовые и иные меры по предотвращению угроз ИБ.

***Безопасность информации***– защищенность информации от нежелательного ее разглашения, искажения, утраты или снижения степени доступности информации.

***Информационная безопасность*** *–* все аспекты, связанные с достижением и поддержанием конфиденциальности, целостности, доступности информации:

*конфиденциальность* - доступен только тем субъектам, которым предоставлены соответствующие полномочия;

*целостность* – может быть модифицирован только субъектом, имеющим для этого соответствующие права.

*доступность* - имеющий соответствующие полномочия субъект может в любое время получить доступ к необходимому ресурсу.