Кононов Д. С .

ВПР31

**Компьютер, хранящий конфиденциальную информацию о разработках предприятия.**

1. Компьюютер — устройство или система, способная выполнять заданную, чётко определённую, изменяемую последовательность операций. Это чаще всего операции численных расчётов и манипулирования данными, однако сюда относятся и операции ввода-вывода.

Конфиденциальность — это комплекс мер по предотвращению утечки и разглашения той или иной информации.

Разработка программного обеспечения — это род деятельности и процесс, направленный на создание и поддержание работоспособности, качества и надежности [программного обеспечения](https://dic.academic.ru/dic.nsf/ruwiki/3647), используя технологии, методологию и практики из [информатики](https://dic.academic.ru/dic.nsf/ruwiki/1147), [управления проектами](https://dic.academic.ru/dic.nsf/ruwiki/48137), [математики](https://dic.academic.ru/dic.nsf/ruwiki/750), [инженерии](https://dic.academic.ru/dic.nsf/ruwiki/940092) и других областей знания.

2. Характер происхождения угроз:

2.1 Случайные факторы – отказы или сбои аппаратуры, программ, систем питания и жизнеобеспечения, стихийные бедствия, несчастные случаи, электромагнитная несовместимость.

2.2 Умышленные факторы – диверсия, непосредственные действия над носителем, информационное воздействие, отказы обслуживания персонала, сбои или ошибки людей

3. Классы каналов несанкционированного доступа:

3.1 Хищение носителей информации

3.2 Копирование информации с носителей

3.3 Установка закладных устройств в помещении и съём информации с их помощью

3.4 Фотографирование или видео съёмка носителей информации внутри помещения

4. Источники появления угроз

4.1 Человеческий фактор

4.2 Аппаратные устройства

4.3 Программное обеспечение

5. Причины нарушения целостности

Непреднамеренные:

5.1 Отказы или сбои аппаратуры, программ, систем питания и жизнеобеспечения

5.2 Стихийные бедствия

5.3 Несчастные случаи

5.4 Электромагнитная несовместимость

Преднамеренные:

5.5 Хищение носителей информации

5.6 Копирование информации с носителей

5.7 Установка закладных устройств в помещении и съём информации с их помощью

5.8 Фотографирование или видео съёмка носителей информации внутри помещения

6. Потенциально возможные злоумышленные действия

6.1 Подключения к линиям связи

6.2 Осмотр отходов мусора

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Целостность | | | | |
| Внешние | | внутренние | | |
| преднамеренные | непреднамеренные | | преднамеренные | непреднамеренные |
| Диверсия | Неисправность оборудования | | Хищение | Ошибки персонала |
| Информационное воздействие | Стихийные бедствия | | Подмена носителей |  |
|  |  | | Уничтожение информации/носителя |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Доступность | | | | |
| Внешние | | внутренние | | |
| преднамеренные | непреднамеренные | | преднамеренные | непреднамеренные |
| Вирус | Сбои работы ПК | | Нанесение ущерба оборудованию сотрудником, имеющим к нему доступ | Сбои в процессе обработки информации |
| Взлом | Сбои работы ПО | | Модификация ПО сотрудником, имеющим к нему доступ | Использование установленного оборудования |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Конфиденциальность | | | | |
| Внешние | | Внутренние | | |
| Преднамерен | Непред | | Пред | Непред |
| Копирование информации | Сбой хранения данных | | Разглашение конф. информации | Невнимательность админа |
|  | Сбой исп. ПО, не зависящего от самого сервера | | Преднамеренное снижение безопасности информации | Потеря информации из-за несовершенного ПО |
|  |  | | Копирование инфы | Ошибки персонала |