

Викторина

«Найди угрозу!»

Для каждой проблемной ситуации:

1. Определить тип угрозы: конфиденциальность, целостность, доступность.
2. Назвать саму угрозу (например, «фишинг», «DDoS-атака», «человеческий фактор»).
3. Предложить краткие меры противодействия угрозе.





Ситуация 1. «Бесплатный Wi-Fi»

Сотрудник бухгалтерии Анна, находясь в командировке, в аэропорту подключилась к открытой публичной сети Wi-Fi с названием «Free_Airport_WiFi», чтобы срочно отправить финансовый отчет директору. Через несколько дней выяснилось, что данные отчета стали известны конкурентам.



Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.

**Конфиденциальность. Угроза: перехват данных в незащищенной сети.
Защита: шифрование трафика, использование VPN**



Ситуация 2. «Инвентарь с сюрпризом»

Студент принес в колледж флеш-накопитель, который нашел в парке. Чтобы найти владельца, он вставил ее в компьютер в учебном классе. Через несколько минут компьютеры в классе перестали отвечать на команды, а на экранах появилось сообщение с требованием выплатить выкуп за разблокировку.



Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.

Доступность, целостность. Угроза: заражение шифровальщиком. Защита: запрет на использование посторонних носителей, антивирусное ПО



Ситуация 3. «Слишком простой пароль»

Системный администратор установил для всех сотрудников компании простой и единый пароль «123456» для входа в корпоративную систему учета. Один из сотрудников был уволен, но через неделю в системе стали появляться несанкционированные изменения в данных о клиентах.



Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.

Конфиденциальность, целостность. Угроза: неавторизованный доступ из-за слабой политики паролей. Защита: строгая политика паролей, немедленное отключение учетных записей уволенных сотрудников



Ситуация 4. «Фишинговая удочка»

Секретарю Марии на рабочую почту пришло письмо от имени «технической поддержки банка» с просьбой «срочно подтвердить данные карты», чтобы разблокировать онлайн-доступ. В письме была ссылка на сайт, внешне неотличимый от сайта банка. Мария ввела свои логин и пароль от банковского приложения.



Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.

Конфиденциальность. Угроза: фишинг. Защита: обучение сотрудников, проверка URL-адресов, двухфакторная аутентификация



Ситуация 5. «Серверная без присмотра»

В серверную комнату колледжа, где хранятся все данные студентов и расписания, может зайти любой человек, так как дверь часто оставляют приоткрытой для «проветривания». Уборщица, протирая пыль, случайно задела кабель питания и главный сервер выключился

Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.



Доступность. Угроза: необеспечение физической безопасности. Защита: Контроль доступа в серверную (пропуска, замки)



Ситуация 6. «Несохраненные изменения»

Преподаватель Петр Иванович неделю работал над новым учебным пособием, сохраняя его на жесткий диск своего компьютера. Во время грозы произошел скачок напряжения, компьютер выключился, и файл с пособием оказался поврежденным и нечитаемым.

Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.



Целостность, доступность. Угроза: Потеря данных из-за сбоя оборудования/электропитания. Защита: Регулярное резервное копирование на внешние носители/в облако, использование источников бесперебойного питания



Ситуация 7. «Ошибка в коде»

Программист Василий при обновлении программного обеспечения интернет-магазина допустил ошибку в программе, отвечающем за расчет скидок. В результате все товары в магазине стали стоить 1 рубль, и за 10 минут было оформлено несколько тысяч заказов.

Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.



Целостность. Угроза: непреднамеренная ошибка персонала, ведущая к нарушению целостности данных. Защита: тестирование кода на тестовом стенде.



Ситуация 8. «Бывший друг»

После ссоры с другом студентка Оля, желая навредить, зашла в его аккаунт в социальной сети (она знала пароль, так как они были в близких отношениях) и удалила все его фотографии и переписку за несколько лет.

Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.



Доступность, целостность. Угроза: злонамеренные действия инсайдера (человека, которому были доверены данные). Защита: не передавать пароли, использовать двухфакторную аутентификацию, регулярно создавать резервные копии



Ситуация 9. «Атака извне»

Сайт колледжа внезапно перестал открываться. Системный администратор обнаружил, что на сервер сайта поступает огромное количество ложных запросов с тысяч разных компьютеров по всему миру, перегружая его и делая недоступным для настоящих абитуриентов.

Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.



Доступность. Угроза: DDoS-атака (Distributed Denial of Service). Защита: использование сервисов защиты от DDoS, настройка сетевых экранов



Ситуация 10. «Слишком много прав»

Все сотрудники отдела продаж имели полный доступ на редактирование и удаление любых данных в общей клиентской базе. Один из стажеров по ошибке отфильтровал и удалил раздел с клиентами, приняв его за тестовые данные.

Какие принципы информационной безопасности были нарушены? Назовите угрозу и способ защиты.



Целостность, доступность. Угроза: Отсутствие разграничения прав доступа. Защита: Внедрение системы ролевого доступа, при которой сотрудники имеют права только на то, что необходимо для их работы.