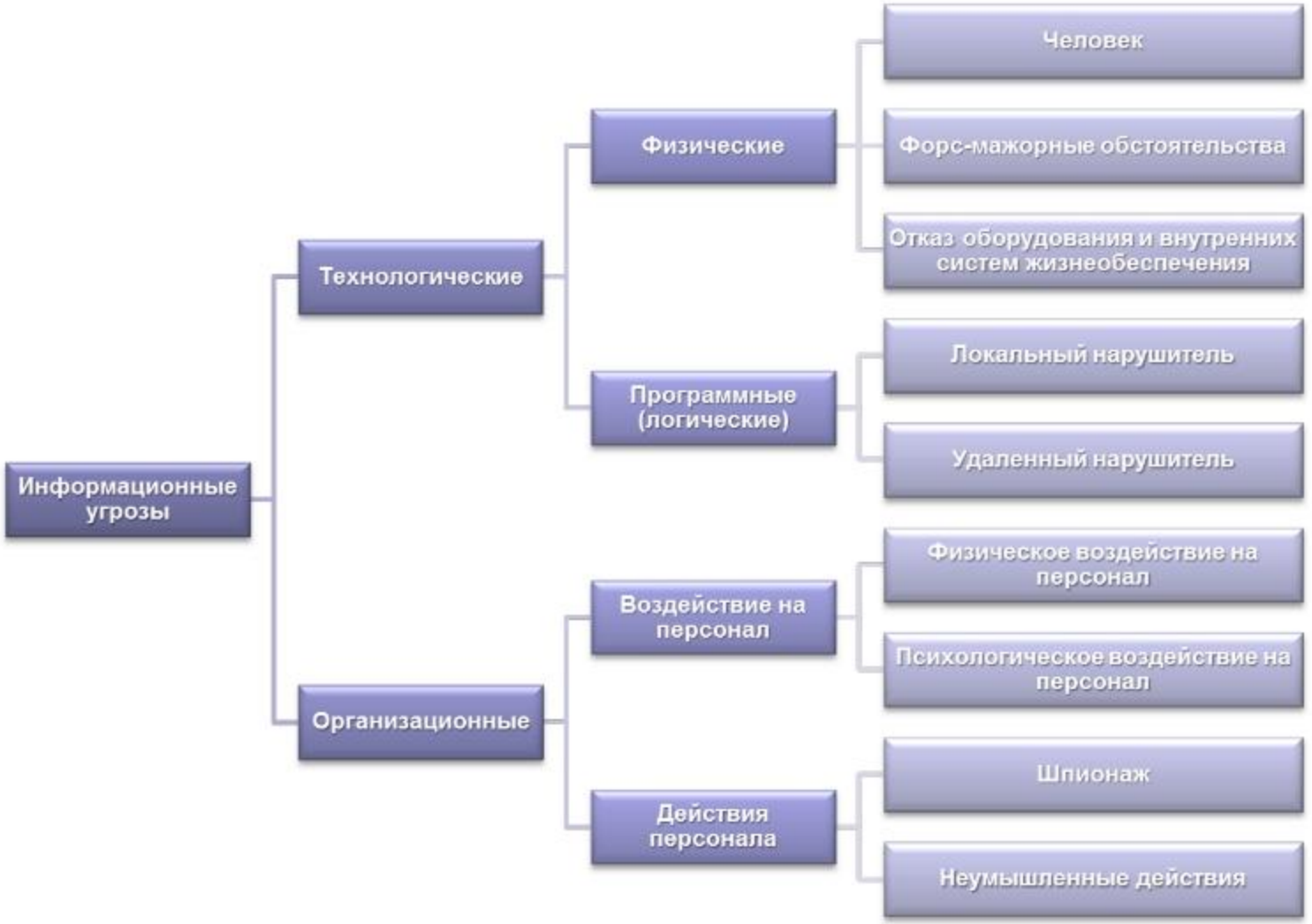
«Информационная безопасность»

Виды информационных угроз



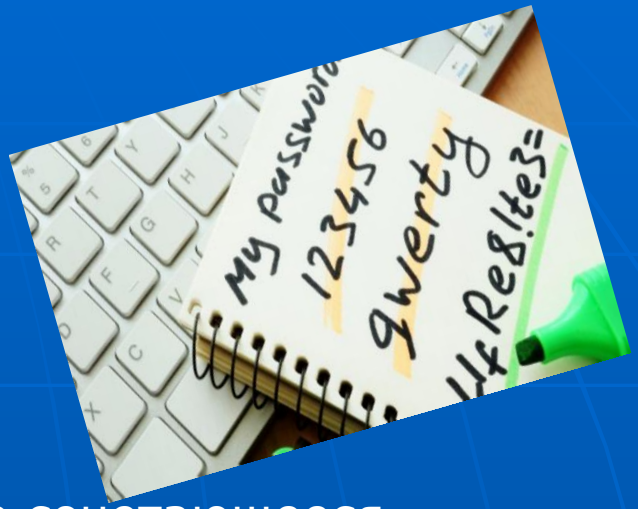
Что может сделать злоумышленник имея логин и пароль:

1. Если вы пользуетесь системами оплаты через интернет, то воспользовавшись вашим логином или паролем, злоумышленник украдет ваши деньги.

2. Злоумышленник может получать деньги за рассылку спама, организовать с вашего компьютера DDOS-атаку . Вы оплачиваете
лишний трафик, миритесь с медленной работой компьютера, возможно общение со службой безопасности атакованной организации.

3. С вашего компьютера может распространяться вирус на компьютеры
ваших знакомых, среди которых найдется тот, на ком можно заработать.

Алгоритмы создания надежных паролей:



Алгоритм 1:
создания сложных паролей:
Выбираем любое прилагательное.
Например «отмороженный»
Выбираем любое существительное, логически не сочетающееся «камень»
Любую легко запоминающуюся цифру (г.р., последние цифры тел. и т.п.)
Любой знак препинания !
Запишем все без пробелов «отмороженныйкамень1998!»
Поменяем одну букву на прописную « отмороженныйКамень1998!» **Алгоритм 2:**
Использовать только вам известное словосочетание «Моя мама готовит вкусные булочки по 12 штук».
Взять первую букву каждого слова «Ммгвбп12ш

ПРОСТЫЕ СОВЕТЫ ПО БЕЗОПАСНОСТИ ПАРОЛЯ

Включайте цифры и символы

Врите, когда отвечаете на секретные вопросы

Используйте менеджер паролей

Регулярно меняйте свой пароль

Используйте фразу из 8 слов для создания пароля-кода

LE VPN

ИНТЕРНЕТ ПО ВАШИМ ПРАВИЛАМ

Памятка
Информационная безопасность

1.Соблюдайте сновные меры компьютерной безопасности: обновления антивирусных программ, обновления программмного обеспечения.

2. Не открывайте файлы, полученные от неизвестных корреспондентов.

3.Принимайте необходимые меры предосторожности, ползуясь беспроводной связью.

4. Создайте пароль, защищающий ваш компьютер и блокирующий возможность его использования.

5. Делайте резервные копии результатов работы.

6. При общении использовать только имя или псевдоним.

7. Номер телефона, свой адрес, место учебы нельзя никому сообщать.

8.Не пересылайте свои фотографии.

9.Без контроля взрослых не встречатьсяс людьми, знакомства с которым завязалось в сети.

10. Доверяйте интуиции.При малейших признаках беспокойства, рассказывайте взрослым.

11. Знайте, что далеко не все, что можно увидеть в Интернете - правда.При сомнении обратитесь к взрослым.