Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный технический университет имени Н.Э. Баумана»
(МГТУ им. Н.Э. Баумана)

Основы обеспечения информационной безопасности

Анализ уязвимостей технологий автоматизации системы «умный дом»

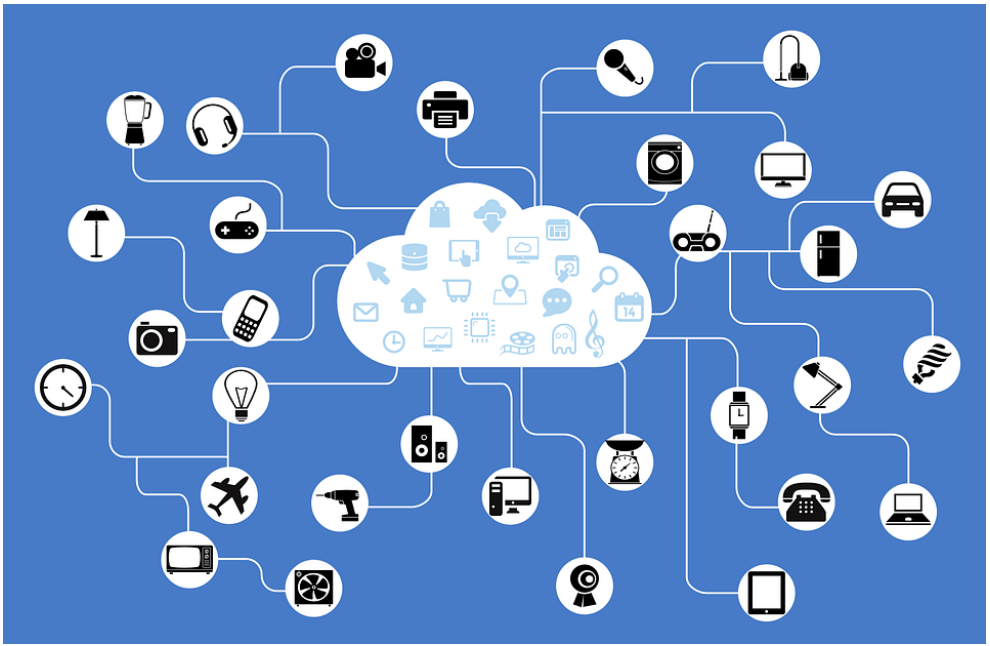
Кафедра «Защита информации»

Интеллектуальная система «Умный дом» — это высокотехнологичная система, позволяющая объединить все коммуникации в одну и поставить её под управление искусственного интеллекта, программируемого и настраиваемого под все потребности и пожелания хозяина.

Типы устройств умного дома:

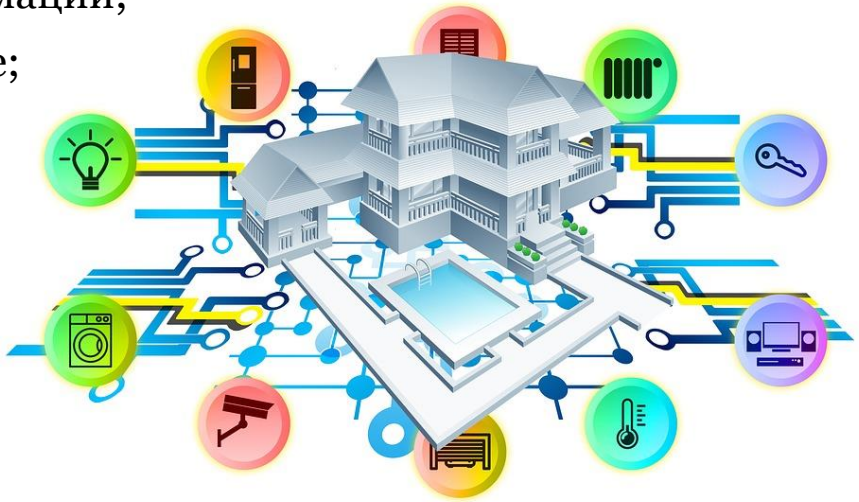
- ✓ Климатическая система;
- ✓ Система освещения;
- ✓ Система безопасности;
- ✓ Солнцезащита;
- ✓ Управление техникой;
- ✓ Энергопотребление и энергосбережение.

Интернет вещей (англ. Internet of Things, IoT) - концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой.



Основные угрозы для системы «умный дом»:

1) Утечка информации через ПЭМИН.
2) Доступ злоумышленника, в связи с кражей прав;
3) Атака хакеров;
4) Перехват информации;
5) Вирусы в системе;



Уязвимость - недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

Основные уязвимости системы «умный дом»:

1. Подключение сети «Умного дома» к Интернету. Таким образом при неэффективной защите могут появляться вирусные программы, а так же повышается вероятность атаки хакеров.

2. При неэффективной защите трафика, повышается вероятность перехвата информации по каналам связи;

3. При плохой системе аутентификации и идентификации возможен доступ несанкционированного пользователя за счет хищения данных;

4. Выход проводников, в которых могут быть наводки излучений, за пределы контролируемой зоны.

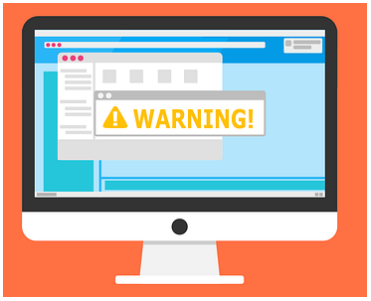
Возможные последствия угроз:

1. Нарушение работы, либо выход из строя центрального сервера, а следовательно и всей системы. Нарушение конфиденциальности, целостности и доступности информации (КЦД).

2. Нарушение конфиденциальности информации, передаваемой по каналу. Возможен захват управления системой.

3. Сбои в ПО системы, а, следовательно, нарушение работы либо вывод из строя аппаратуры системы. Нарушение КЦД информации, находящейся внутри сети.

4. Нарушение конфиденциальности информации, обрабатываемой на ЭВМ.

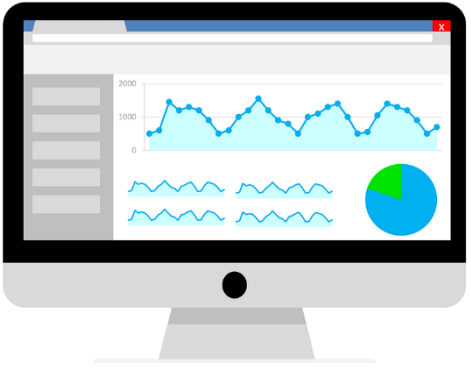


Оценка влияния угрозы

Высокое влияние на систему (ВВ) - влияние на конфиденциальность, целостность и доступность элементов системы может причинить организации (владельцам) значительный или катастрофический ущерб.

Среднее влияние на систему (СВ) - влияние на конфиденциальность, целостность и доступность элементов системы может причинить организации (владельцам) средний ущерб. Средний ущерб не вызывает значительных или катастрофических изменений, однако нарушает нормальную работу организации (нормальную жизнедеятельность).

Низкое влияние на систему (НВ) – влияние на конфиденциальность, целостность и доступность элементов системы не причиняет организации (владельцам) какого – либо серьезного ущерба.

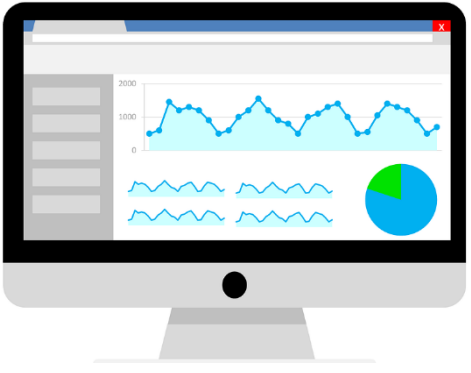


Степень подверженности воздействию

1. **Высокая подверженность воздействию.** Значительный или полный ущерб для актива.

2. **Средняя подверженность воздействию.** Средний или ограниченный ущерб.

3. **Низкая подверженность воздействию.** Незначительный ущерб или отсутствие такового.



Оценка вероятности угроз

Уровни в списке с обобщенными сведениями о рисках

Влияние (из предыдущей таблицы)				
	Выс.	Средн.	Выс.	Выс.
	Средн.	Низк.	Средн.	Выс.
	Низк.	Низк.	Низк.	Средн.
		Низк.	Средн.	Выс.
		Уровень вероятности