Раздел: Жизненный цикл ИБ
Модуль 4: Целенаправленные атаки. Модуль Практическое задание. Определение актуальных угроз по методологии ФСТЭК России.
Выполнил: Александр Ганицев

У**словия задачи.**

Дана коммерческая организация, которая занимается грузоперевозками. В организации работает несколько отделов:

– менеджеры по грузоперевозкам,
– бухгалтерия,
– кадровая служба,
– служба ИТ.

Дополнительная информация:

– есть сайт, размещённый на собственных мощностях;
– DMZ-зона отсутствует;
– удалённых сотрудников нет;
– менеджеры звонят с использованием IP-телефонии.

Что нужно сделать.

Ваша задача — на основе данных об организации продумать сценарии реализации угроз безопасности информации по методологии ФСТЭК России, а также выделить угрозы из БДУ ФСТЭК, которые реализуются благодаря этому сценарию.

Предоставьте ответ в таблице формата:

№ п/п	Номер из БДУ ФСТЭК	Наименование угрозы безопасности информации	Сценарии реализации угроз (допускается использовать коды из методики определения угроз)
1	УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Т1.1, Т2.2

Критерии оценивания ментором.

Максимальное количество баллов — 5.

5 — указаны угрозы несанкционированного доступа к информации, угрозы веб-приложений, угрозы перехвата каналов связи, угрозы вирусных атак.

4 — указаны три из четырёх видов угроз: несанкционированный доступ к информации, угрозы веб-приложений, угрозы перехвата каналов связи, угрозы вирусных атак.

3 — приведены два из четырёх видов угроз.

2 — приведён один из четырёх видов угроз.

1 — приведены другие угрозы, не относящиеся к списку выше.

0 — ничего не сделано.

Выполнение.

№ п/п	Номер из БДУ ФСТЭК	Наименование угрозы безопасности информации	Сценарии реализации угроз (допускается использовать коды из методики определения угроз)
1	УБИ. 073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Т1.1, Т2.2, Т2.5
2	УБИ. 173	Угроза «спама» веб-сервера	Т1.1, Т1.5, Т2.1, Т2.5
3	УБИ. 069	Угроза неправомерных действий в каналах связи	Т1.14, Т2.9
4	УБИ. 001	Угроза автоматического распространения вредоносного кода в грид-системе	Т3.3, Т3.6
5	УБИ. 186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Т1.11, Т2.5
6	УБИ. 190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Т2.5
7	УБИ. 195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Т2.4., Т2.7, Т3.4