Министерство образования Российской Федерации

Пензенский государственный университет

Кафедра «САПР»

**ОТЧЁТ**

По лабораторной работе №4

По курсу «Информационная безопасность САПР»

На тему «Предпроектная стадия обследование объекта информатизации»

Выполнил:

ст. гр.20ВВ2.1

Горбунов Никита

Проверила:

Эпп В. В.

Пенза 2022

Модель ИСПД:

ПК

ИНТЕРНЕТ

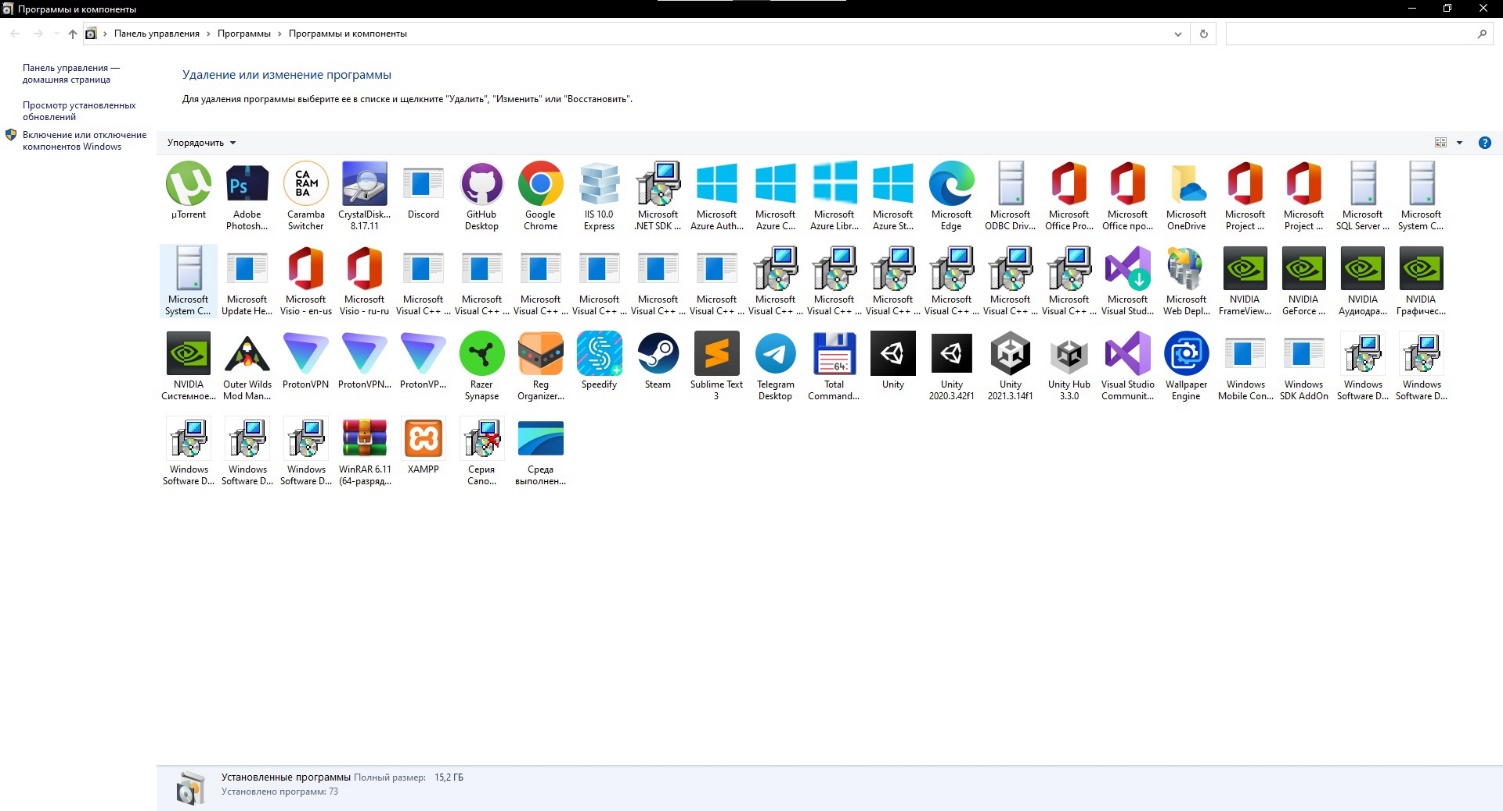
РОУТЕР

НОУТБУК

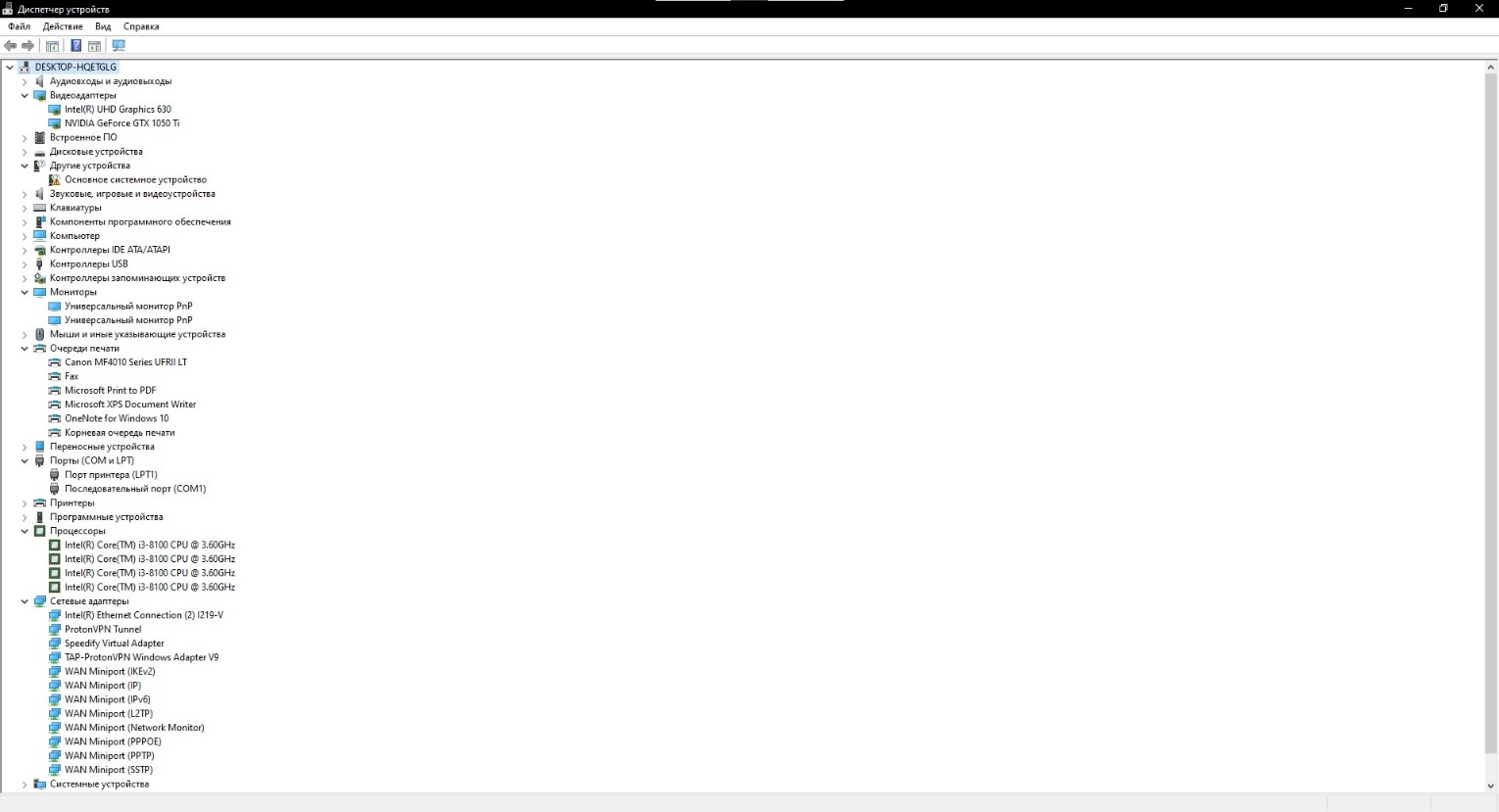
Таблица A – Показатели исходной защищенности ИСПДн

|  |  |  |  |
| --- | --- | --- | --- |
| Технические и эксплуатационные характеристики ИСПДн | Уровень защищенности | | |
| Высокий | Средний | Низки й |
| **1. По территориальному размещению:** |  | | |
| в пределах одного здания | **+** | **–** | **–** |
| **2. По наличию соединения с сетями общего пользования:** |  | | |
| многоточечный выход в  сеть общего пользования | **–** | **–** | **+** |
| **3. По встроенным (легальным) операциям с записями баз персональных данных:** |  | | |
| модификация, передача | **–** | **–** | **+** |
| **4. По разграничению доступа к персональным данным:** |  | | |
| ограниченный круг лиц | **–** | **+** | **–** |
| **5. По наличию соединений с другими базами ПДн иных ИСПДн:** |  | | |
| нет | **–** | **–** | **–** |
| **6. По уровню обобщения (обезличивания) ПДн:** |  | | |
| данные обезличиваются при передаче другим пользователям, но не обезличиваются при передаче между моими устройствами | **–** | **+** | **–** |
| **7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:** |  | | |
| предоставляющая часть | **–** | **+** | **–** |
| **Исходная степень защищенности (Y1)** | **Средняя** | | |

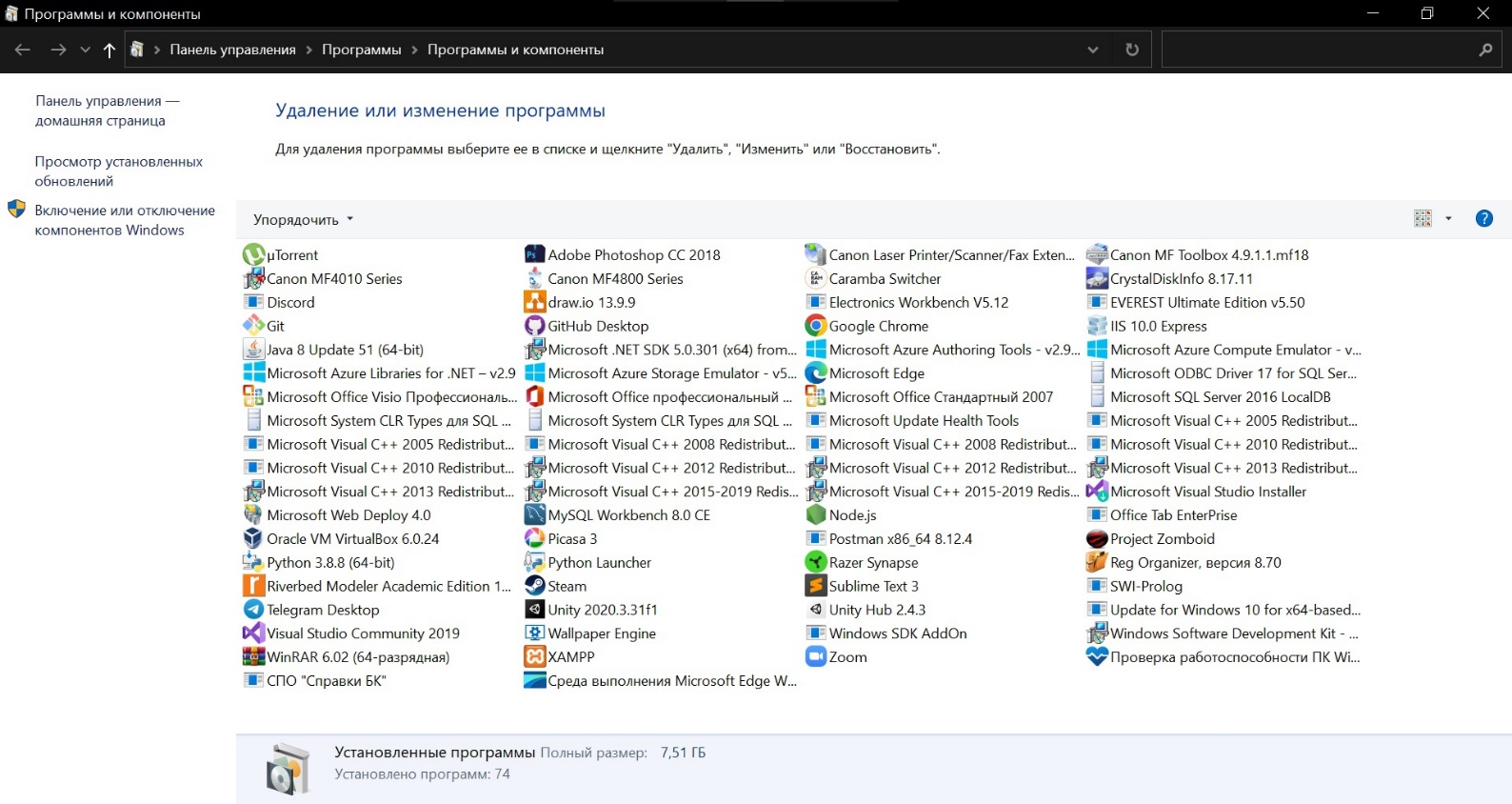
Программы и компоненты ПК:



Диспетчер устройств ПК:



Программы и компоненты ноутбука:



Диспетчер устройств ноутбука:

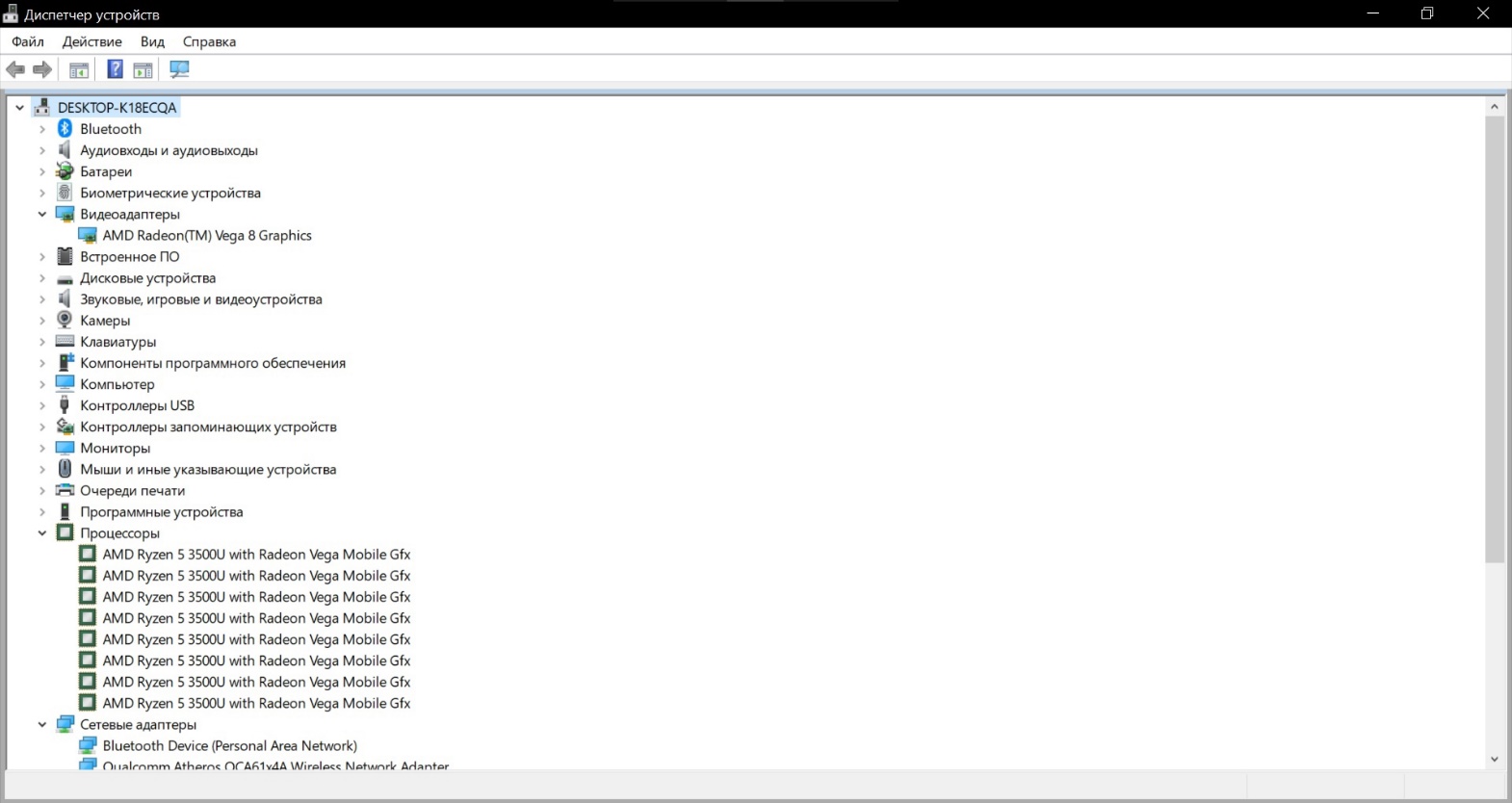


Таблица B – Итоговая модель угроз безопасности ПДн

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование угрозы | Вероятность реализации угрозы (Y2) | Возможность реализации угрозы (Y) | Опасность угрозы | Актуальность угрозы |
| 1 Угрозы от утечки по техническим каналам | | | | |
| 1.1 Угрозы утечки акустической (речевой) информации | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 1.2 Угрозы утечки  видовой информации | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 1.3 Угрозы утечки информации по каналам  ПЭМИН | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 2 Угрозы несанкционированного доступа к информации | | | | |
| 2.1 Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | | | | |
| 2.1.1 Кража ПЭВМ | Низкая вероятность | Низкая | Высокая | Актуальная |
| 2.1.2 Кража носителей  Информации | Низкая вероятность | Низкая | Высокая | Актуальная |
| 2.1.3 Кража ключей  Доступа | Низкая вероятность | Низкая | Высокая | Актуальная |
| 2.1.4 Кражи, модификации, уничтожения информации | Низкая вероятность | Низкая | Высокая | Актуальная |
| 2.1.5 Вывод из строя узлов ПЭВМ, каналов связи | Низкая вероятность | Низкая | Высокая | Актуальная |
| 2.1.6 Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 2.1.7 Несанкционированное отключение средств защиты | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и  программных средств (в том числе программно-математических воздействий) | | | | |
| 2.2.1 Действия  вредоносных программ (вирусов) | Средняя  вероятность | Высокая | Средняя | Актуальная |
| 2.2.2 Установка ПО, не связанного с исполнением служебных обязанностей | Низкая вероятность | Низкая | Средняя | Актуальная |
| 2.2.3 Перехват паролей  или идентификаторов | Средняя  вероятность | Средняя | Высокая | Актуальная |
| 2.2.4 Модификация базовой системы ввода/вывода (BIOS) | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 2.2.5 Перехват управления загрузкой | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 2.2.6 Использование остаточной информации,  «сбор мусора» | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 2.2.7 Программно-  аппаратная закладка | Низкая вероятность | Низкая | Средняя | Неактуальная |
| 2.2.8 Программная  закладка | Низкая вероятность | Низкая | Средняя | Неактуальная |
| 2.2.9  Недекларированные возможности в системном программном обеспечении | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 2.2.10 Недекларированные возможности в прикладном программном обеспечении | Низкая вероятность | Низкая | Низкая | Неактуальная |
| 2.3 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера | | | | |
| 2.3.1 Утрата ключей и  атрибутов доступа | Низкая  вероятность | Низкая | Высокая | Актуальная |
| 2.3.2 Непреднамеренная модификация (уничтожение) информации сотрудниками | Низкая  вероятность | Средняя | Высокая | Актуальная |
| 2.3.3 Непреднамеренное отключение средств защиты | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.3.4 Выход из строя аппаратно-программных  средств | Низкая  вероятность | Средняя | Средняя | Актуальная |
| 2.3.5 Сбой системы  электроснабжения | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.3.6 Стихийное бедствие | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.4 Угрозы преднамеренных действий нарушителей | | | | |
| 2.4.1 Доступ к информации, модификация, уничтожение лицами не допущенных к ее  обработке | Низкая  вероятность | Низкая | Средняя | Неактуальная |
| 2.4.2 Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.5 Угрозы несанкционированного доступа по каналам связи (в пределах контролируемой зоны) | | | | |
| 2.5.1 Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей  информации | Низкая вероятность | Средняя | Средняя | Актуальная |
| 2.5.2 Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых  соединений и др. | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.5.3 Угрозы выявления  паролей по сети | Средняя  вероятность | Средняя | Средняя | Актуальная |
| 2.5.4 Угрозы подмены доверенного объекта в  сети | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.5.5 Угрозы типа «Отказ  в обслуживании» | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.5.6 Угрозы удаленного  запуска приложений | Низкая  вероятность | Низкая | Средняя | Неактуальная |
| 2.5.7 Угрозы внедрения  по сети вредоносных программ | Низкая  вероятность | Низкая | Средняя | Неактуальная |
| 2.6 Угрозы несанкционированного доступа по каналам связи (за пределами контролируемой зоны) | | | | |
| 2.6.1 Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей  информации | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.6.2 Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и  служб, открытых соединений и др. | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.6.3 Угрозы выявления  паролей по сети | Средняя  вероятность | Средняя | Средняя | Актуальная |
| 2.6.4 Угрозы подмены  доверенного объекта в сети | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.6.5 Угрозы типа «Отказ  в обслуживании» | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.6.6 Угрозы удаленного  запуска приложений | Низкая  вероятность | Низкая | Средняя | Неактуальная |
| 2.6.7 Угрозы внедрения по сети вредоносных  программ | Низкая  вероятность | Низкая | Средняя | Неактуальная |

- возможность реализации угрозы признается средней