Министерство образования Российской Федерации

Пензенский государственный университет

Кафедра «Системы автоматизированного проектирования»

**Отчет**

По лабораторной работе №1

По курсу «Информационная безопасность САПР»

На тему «Предпроектная стадия. Обследование объекта информатизации»

Выполнил студент гр.20ВВ2.1

Горбунов Н.А.

Проверили:

Епп В.В.

Пенза, 2022

**Цель**

Исследовать персональный компьютер для дальнейшей защиты информации.

**Обследование объекта информатизации:**Объект информатизации: ноутбук.

**Система обработки ПД**Файловая система, программа обработки текстовых файлов, программа обработки таблиц, САПР программа, среда разработки.

1. структура ИСПДн:
   1. автономные ИСПДн АРМ;
   2. локальные ИСПДн:
   3. распределенные ИСПДн):
2. категория обрабатываемых в ИСПДн персональных данных:
   1. ИСПДн-И;
3. Объем обрабатываемых в ИСПДн персональных данных:
   1. менее чем 100 000 субъектов;
4. наличие подключений ИСПДн к сетям связи общего пользования/сетям МИО:
   1. не имеющие подключение;
   2. имеющие подключение.
5. характеристики подсистемы безопасности ИСПДн;
6. режимы обработки персональных данных:
   1. многопользовательские ИСПДН.
7. режимы разграничения прав доступа пользователей ИСПДн:
   1. с разграничением доступа;
   2. без разграничения доступа;
8. условия размещения технических средств ИСПДн:
   1. в пределах контролируемой зоны;
9. по территориальному размещению:
   1. локальная ИСПДн, развернутая в пределах одного здания.

|  |  |  |  |
| --- | --- | --- | --- |
| Технические и эксплутационные характеристики ИСПДи | Уровень защищенности | | |
| Высокий | Средний | Низкий |
| По территориальному размещению: |  | + |  |
| По наличию соединения с сетями общего пользования: |  |  | + |
| По встроенным (легальным) операциям с записями баз персональных данных |  |  | + |
| По разграничению доступа к персональным данным: |  |  |  |
| По наличию соединений с другими базами ПДн иных ИСПДн |  |  |  |
| По уровню обобщения (обезличивания) ПДн |  |  |  |
| По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки |  |  |  |
| РЕЗУЛЬТАТ (Y1) |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | Маловероятно | Низкая | Низкая | Неактуальная |
| 1.2 Угрозы утечки  видовой информации | Средняя  вероятность | Средняя | Низкая | Неактуальная |
| 1.3 Угрозы утечки информации по каналам  ПЭМИН | Средняя 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 | Средняя  вероятность | Высокая | Высокая | Актуальная |
| 2.1.2 Кража носителей  Информации | Высокая  вероятность | Высокая | Средняя | Актуальная |
| 2.1.3 Кража ключей  Доступа | Низкая  вероятность | Низкая | Средняя | Неактуальная |
| 2.1.4 Кражи, модификации, уничтожения информации | Средняя вероятность | Средняя | Средняя | Актуальная |
| 2.1.5 Вывод из строя узлов ПЭВМ, каналов  Связи | Средняя  вероятность | Низкая | Низкая | Неактуальная |
| 2.1.6  Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Средняя вероятность | Низкая | Низкая | Неактуальная |
| 2.1.7  Несанкционированное отключение средств защиты | Маловероятно | Низкая | Высокая | Актуальная |
| 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 | Высокая | Актуальная |
| 2.2.2 Установка ПО, не связанного с  исполнением служебных обязанностей | Средняя вероятность | Высокая | Высокая | Актуальная |
| 2.2.3 Перехват паролей  или идентификаторов | Высокая  вероятность | Средняя | Высокая | Актуальная |
| 2.2.4 Модификация базовой системы  ввода/вывода (BIOS) | Низкая вероятность | Средняя | Средняя | Актуальная |
| 2.2.5 Перехват  управления загрузкой | Маловероятно | Низкая | Низкая | Неактуальная |
| 2.2.6 Использование остаточной информации,  «сбор мусора» | Маловероятно | Низкая | Низкая | Неактуальная |
| 2.2.7 Программно-  аппаратная закладка | Маловероятно | Низкая | Средняя | Неактуальная |
| 2.2.8 Программная  закладка | Маловероятно | Низкая | Средняя | Неактуальная |
| 2.2.9  Недекларированные возможности в системном программном обеспечении | Низкая вероятность | Низкая | Средняя | Неактуальная |
| 2.2.10  Недекларированные возможности в прикладном программном обеспечении | Низкая вероятность | Низкая | Средняя | 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 | Средняя  вероятность | Средняя | Средняя | Актуальная |
| 2.3.2 Непреднамеренная модификация (уничтожение) информации  сотрудниками | Маловероятно | Средняя | Высокая | Актуальная |
| 2.3.3 Непреднамеренное отключение средств  защиты | Маловероятно | Низкая | Высокая | Актуальная |
| 2.3.4 Выход из строя аппаратно-программных  средств | Низкая  вероятность | Средняя | Низкая | Актуальная |
| 2.3.5 Сбой системы  электроснабжения | Маловероятно | Низкая | Низкая | Неактуальная |
| 2.3.6 Стихийное  бедствие | Маловероятно | Низкая | Низкая | Неактуальная |
| 2.4 Угрозы преднамеренных действий нарушителей | | | | |
| 2.4.1 Доступ к информации, модификация, уничтожение лицами не допущенных к ее  обработке | Средняя вероятность | Средняя | Средняя | Актуальная |
| 2.4.2 Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее  обработке | Низкая  вероятность | Средняя | 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 | Средняя 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 | Высокая | Актуальная |
| 2.5.4 Угрозы подмены доверенного объекта в  сети | Маловероятно | Низкая | Низкая | Неактуальная |
| 2.5.5 Угрозы типа «Отказ  в обслуживании» | Низкая  вероятность | Низкая | Низкая | Неактуальная |
| 2.5.6 Угрозы удаленного  запуска приложений | Маловероятно | Низкая | Низкая | Неактуальная |
| 2.5.7 Угрозы внедрения  по сети вредоносных программ | Низкая  вероятность | Средняя | Средняя | Актуальная |
| 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 | Высокая | 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 | Маловероятно | Низкая | Низкая | Неактуальная |
| 2.6.7 Угрозы внедрения по сети вредоносных  программ | Низкая  вероятность | Средняя | Средняя | Актуальная |

РЕЗУЛЬТАТ (*Y1*)