ПРОЕКТ

**ПРАВИТЕЛЬСТВО РОСТОВСКОЙ ОБЛАСТИ**

**ДЕПАРТАМЕНТ ПОТРЕБИТЕЛЬСКОГО РЫНКА**

**РОСТОВСКОЙ ОБЛАСТИ**

**П О С Т А Н О В Л Е Н И Е**

|  |  |  |
| --- | --- | --- |
| «\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_ | № \_\_\_\_\_\_ | г. Ростов-на-Дону |

Об утверждении перечня актуальных угроз

безопасности персональных данных

в информационной системе персональных

данных департамента потребительского

рынка Ростовской области.

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006

№ 152-ФЗ «О персональных данных» департамент потребительского рынка Ростовской области **п о с т а н о в л я е т:**

1. Утвердить Перечень актуальных угроз безопасности персональных данных в информационной системе персональных данных департамента потребительского рынка Ростовской области.
2. Контроль за выполнением настоящего постановления оставляю за собой.

Директор департамента И.В. Теларова

Приказ вносит отдел лицензирования

Приложение

к постановлению департамента потребительского рынка Ростовской области

от «\_\_\_»\_\_\_\_\_\_2017 г. № \_\_\_\_

Перечень актуальных угроз безопасности персональных данных в информационной системе персональных данных департамента потребительского рынка Ростовской области.

Согласно акту определения угроз безопасности персональных данных в информационной системе персональных данных департамента потребительского рынка Ростовской области (далее – ИСПДн) актуальны следующие угрозы:

утечка акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке персональных данных (далее – ПДн) в ИСПДн, возможная при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн;

утечка видовой информации, возможная за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн;

утечка информации по каналу побочных электромагнитных излучений и наводки (далее – ПЭМИН), возможная из-за наличия паразитных электромагнитных излучений у элементов ИСПДн;

кража персональной электронно-вычислительной машины (далее – ПЭВМ), осуществляемая путем несанкционированного доступа к информации (далее – НСД) внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн;

кража носителей информации, осуществляемая путем НСД внешними и внутренними нарушителями к носителям информации;

кража ключей и атрибутов доступа, осуществляемая путем НСД внешними и внутренними нарушителями в помещениях, в которых происходит работа пользователей;

кража, модификация, уничтожение информации, осуществляемые путем НСД внешними и внутренними нарушителями в помещениях, в которых расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей;

вывод из строя узлов ПЭВМ, каналов связи, НСД к узлам ПЭВМ и каналам связи, осуществляемые путем НСД внешними и внутренними нарушителями в помещениях, в которых расположены элементы ИСПДн и проходят каналы связи;

несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ;

несанкционированное отключение средств защиты, осуществляемое путем НСД внешними и внутренними нарушителями в помещениях, в которых расположены средства защиты ИСПДн;

воздействие вредоносных программ (вирусов);

нарушение конфиденциальности, доступности или целостности обрабатываемой информации при возникновении недекларированных возможностей системного программного обеспечения (далее – ПО) и ПО для обработки персональных данных;

установка ПО, не связанного с исполнением служебных обязанностей, осуществляемая путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов;

утрата ключей и атрибутов доступа, осуществляемая за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них;

непреднамеренная модификация, уничтожение информации сотрудниками, осуществляемые за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них;

непреднамеренное отключение средств защиты, осуществляемое за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них;

сбой системы электроснабжения, происходящий вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации;

стихийное бедствие, происходящее вследствие несоблюдения мер пожарной безопасности;

доступ к информации, ее модификация и уничтожение лицами, не допущенными к ее обработке, осуществляемые путем НСД внешних нарушителей в помещениях, в которых расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей;

разглашение информации, ее модификация и уничтожение сотрудниками, допущенными к ее обработке, осуществляемые за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них;

анализ сетевого трафика внешними нарушителями в пределах контролируемой зоны;

анализ сетевого трафика внешними нарушителями за пределами контролируемой зоны;

анализ сетевого трафика внутренними нарушителями;

сканирование сети, реализуемое в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них;

выявление пароля, реализуемое путем использования специальных программ, которые пытаются получить доступ хосту путем последовательного подбора паролей;

навязывание ложного маршрута сети, обусловленное недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств);

подмена доверенного объекта, реализуемая в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д.;

внедрение ложного объекта сети, основанное на использовании недостатков алгоритмов удаленного поиска;

угроза типа «Отказ в обслуживании», основанная на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, в которых операционная система оказывается не в состоянии обрабатывать поступающие пакеты;

удаленный запуск приложений, заключающийся в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы (программы-закладки, вирусы, «сетевые шпионы»), основная цель которых – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста;

внедрение по сети вредоносных программ.