# АДМИНИСТРАЦИЯ ТОМСКОЙ ОБЛАСТИ

# ПОСТАНОВЛЕНИЕ

19.10.2016 № 334а

Об отдельных мерах по обеспечению безопасности персональных данных при их обработке

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

ПОСТАНОВЛЯЮ:

1. Утвердить Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Администрации Томской области, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки согласно приложению к настоящему постановлению.

2. Контроль за исполнением настоящего постановления возложить на заместителя Губернатора Томской области – начальника Контрольно-ревизионного управления Администрации Томской области Шестакова А.В.

И.о. Губернатора Томской области А.М.Рожков

Администрация Томской области ПРОТОКОЛЬНАЯ ГРУППА Управления делами

А.В.Шестаков
1013kv05.pap2016

УТВЕРЖДЕН
постановлением Администрации
Томской области
от 19.10.2016 № 334а

# Перечень
# угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Администрации Томской области, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

1. Угрозы утечки информации по техническим каналам:

1) угрозы утечки акустической (речевой) информации:

угрозы внедрения специальных звукозаписывающих электронных устройств в помещения;

2) угрозы утечки видовой информации:

угрозы утечки видовой информации с экрана дисплеев;

угрозы утечки видовой информации с технических средств;

угрозы обработки графической, видео- и буквенно-цифровой информации;

угрозы внедрения специальных видеозаписывающих электронных устройств в помещения;

3) угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее – ПЭМИН):

угрозы утечки по каналам ПЭМИН информативных сигналов от технических средств и линий передачи информации;

угрозы наводок информативного сигнала на цепи электропитания и линии связи;

угрозы утечки радиоизлучения.

2. Угрозы несанкционированного доступа к информационным системам персональных данных, включающие в себя:

1) угрозы, реализуемые в ходе загрузки операционной системы:

угрозы выявления паролей или идентификатора;

угрозы модификации программного обеспечения базовой системы ввода – вывода (BIOS);

угрозы перехвата управления загрузкой с изменением необходимой технологической информации;

2) угрозы, реализуемые после загрузки операционной системы:

угрозы несанкционированного копирования защищаемой информации, обрабатываемой в информационных системах персональных данных (далее – ИСПДн);

угрозы разглашения (публикации) защищаемой информации, обрабатываемой в ИСПДн;

угрозы разглашения (публикации) состава программно-аппаратных средств ИСПДн;

угрозы разглашения (публикации) состава средств защиты персональных данных (далее – ПДн);

угрозы хищения аппаратных средств и носителей информации;

угрозы несанкционированного отключения средств защиты;

угрозы несанкционированной модификации защищаемой информации, обрабатываемой в ИСПДн;

угрозы несанкционированного уничтожения защищаемой информации, обрабатываемой в ИСПДн;

угрозы несанкционированной модификации конфигурации прикладного и специального программного обеспечения ИСПДн;

угрозы несанкционированного уничтожения прикладного и специального программного обеспечения ИСПДн;

3) угрозы отказа в обслуживании:

угрозы нарушения функционирования и отказ средств обработки ИСПДн;

угрозы нарушения функционирования и отказ средств хранения информации;

угрозы нарушения функционирования и отказ средств защиты информации;

4) угрозы внедрения вредоносных программ:

угрозы внедрения программной закладки;

угрозы внедрения (классического) программного вируса;

угрозы внедрения программной закладки по сети;

угрозы внедрения (классического) программного вируса по сети;

5) угрозы сетевой безопасности:

угрозы выявления паролей;

угрозы анализа сетевого трафика, передаваемого во внешнюю сеть и принимаемого из внешней сети;

угрозы сканирования сети, направленные на определение топологии сети, выявление типа операционной системы, сетевых адресов, открытых портов и запущенных служб;

угрозы модификации конфигурации сети;

угрозы модификации сетевых адресов;

угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

угрозы внедрения ложного объекта сети;

угрозы подмены доверенного объекта в сети;

угрозы скрытого отказа в обслуживании, вызванного привлечением части ресурсов ИСПДн;

угрозы отказа в обслуживании, вызванного передачей злоумышленником пакетов с нетрадиционными атрибутами;

угрозы явного отказа в обслуживании, вызванного исчерпанием ресурсов ИСПДн;

угрозы явного отказа в обслуживании, вызванного нарушением логической связанности между техническими средствами ИСПДн;

угрозы удаленного запуска приложений путем распространения файлов, содержащих несанкционированный исполняемый код;

угрозы удаленного запуска приложений путем использования возможностей удаленного управления системой;

6) угрозы безопасности среды виртуализации:

угрозы перехвата управления средой виртуализации;

угрозы нарушения изоляции пользовательских данных внутри виртуальной машины;

угрозы нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

угрозы нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин;

угрозы несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;

угрозы несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети;

угрозы несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;

угрозы выхода процесса за пределы виртуальной машины;

7) угрозы безопасности использования в информационной системе технологий беспроводного доступа:

угрозы несанкционированного доступа к ИСПДн по беспроводным каналам;

угрозы подключения к беспроводной сети в обход процедуры аутентификации;

угрозы подмены беспроводного клиента или точки доступа.

3. Угрозы недекларированных возможностей программного обеспечения, включающие в себя:

1) угрозы нарушения целостности, конфиденциальности, доступности обрабатываемых персональных данных в ИСПДн с использованием недекларированных возможностей в операционной системе;

2) угрозы нарушения целостности, конфиденциальности, доступности обрабатываемых персональных данных в ИСПДн с использованием недекларированных возможностей в прикладном программном обеспечении.

4. Угрозы нарушителей и направление возможных атак при использовании средств криптографической защиты (далее – СКЗИ):

1) проведение атак на этапе эксплуатации СКЗИ на следующие объекты:

документацию на СКЗИ и компоненты среды функционирования СКЗИ;

помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ;

2) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники (далее – СВТ), на которых реализованы СКЗИ;

3) использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

4) физический доступ к СВТ, на которых реализованы СКЗИ;

5) возможность воздействовать на аппаратные компоненты СКЗИ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

6) создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения;

7) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

8) проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ;

9) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения;

10) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СКЗИ;

11) возможность воздействовать на любые компоненты СКЗИ.