ПРАВИТЕЛЬСТВО ЯМАЛО-НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА

ПОСТАНОВЛЕНИЕ

09 сентября 2016 г. № 837-П

г. Салехард

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учётом содержания персональных данных, характера и способов их обработки и информации, не содержащей сведения, составляющие государственную тайну, реализация которых может привести к нарушению безопасности информации, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах исполнительных органов государственной власти Ямало-Ненецкого автономного округа

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», во исполнение пункта 14.3 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждённых приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 11 февраля 2013 года № 17, с целью обеспечения единого подхода к определению угроз безопасности информации (персональных данных), актуальных для информационных систем исполнительных органов государственной власти Ямало-Ненецкого автономного округа, Правительство Ямало-Ненецкого автономного округа **п о с т а н о в л я е т:**

1. Утвердить прилагаемый перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учётом содержания персональных данных, характера и способов их обработки и информации, не содержащей сведения, составляющие государственную тайну, реализация которых может привести к нарушению безопасности информации, не содержащей сведения,

составляющие государственную тайну, в государственных информационных системах исполнительных органов государственной власти Ямало-Ненецкого автономного округа (далее – перечень).

2. Департаменту информационных технологий и связи Ямало-Ненецкого автономного округа (Ефремов О.В.) в месячный срок со дня вступления в силу настоящего постановления разработать с учётом перечня и утвердить типовую модель угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учётом содержания персональных данных, характера и способов их обработки и информации, не содержащей сведения, составляющие государственную тайну, реализация которых может привести к нарушению безопасности информации, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах исполнительных органов государственной власти Ямало-Ненецкого автономного округа (далее – типовая модель угроз).

3. Исполнительным органам государственной власти Ямало-Ненецкого автономного округа в месячный срок с момента получения утверждённой типовой модели угроз обеспечить разработку модели угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учётом содержания персональных данных, характера и способов их обработки и информации, не содержащей сведения, составляющие государственную тайну, реализация которых может привести к нарушению безопасности информации, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах исполнительных органов государственной власти Ямало-Ненецкого автономного округа, в соответствии с типовой моделью угроз.

4. Рекомендовать органам местного самоуправления муниципальных образований в Ямало-Ненецком автономном округе учитывать перечень в рамках работ по обеспечению безопасности информации, в том числе персональных данных.

5. Контроль за исполнением настоящего постановления возложить на заместителя Губернатора Ямало-Ненецкого автономного округа, руководителя аппарата Губернатора Ямало-Ненецкого автономного округа Фиголь Н.В.

Губернатор
Ямало-Ненецкого автономного округа Д.Н. Кобылкин

Управление по обеспечению деятельности Правительства и Губернатора

УТВЕРЖДЁН

постановлением Правительства
Ямало-Ненецкого автономного округа
от 09 сентября 2016 года № 837-П

ПЕРЕЧЕНЬ

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки и информации, не содержащей сведения, составляющие государственную тайну, реализация которых может привести к нарушению безопасности информации, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах исполнительных органов государственной власти Ямало-Ненецкого автономного округа

№ п/п	Наименование угрозы
1	2
1.	Угрозы утечки информации по техническим каналам
1.1.	Угроза утечки акустической (речевой) информации при наличии функций голосового ввода данных в информационной системе исполнительных органов государственной власти Ямало-Ненецкого автономного округа (далее – ИС, ИС ИОГВ ЯНАО) или функций воспроизведения данных акустическими средствами ИС ИОГВ ЯНАО
1.2.	Угроза утечки видовой информации при условии наличия прямого оптического канала просмотра данных
1.3.	Угроза утечки информации по каналу побочных электромагнитных излучений и наводок для наиболее важных (критичных) информационных систем и баз данных
2.	Угрозы внедрения аппаратных закладок
2.1.	Угроза внедрения аппаратных закладок в серверное оборудование иностранного производства систем управления баз данных наиболее важных (критичных) информационных систем
2.2.	Угроза внедрения аппаратных закладок в серверное оборудование иностранного производства, используемого для работы ИС ИОГВ ЯНАО
3.	Угрозы несанкционированных действий (далее – НСД), связанные с действиями нарушителей, имеющих доступ к техническим средствам ИС ИОГВ ЯНАО
3.1.	Угроза физического уничтожения, повреждения, хищения данных и (или) технических средств (носителей информации) ИС ИОГВ ЯНАО

1	2
3.2.	Угроза безопасности информации, связанная с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении наиболее важных (критичных) информационных систем и баз данных
3.3.	Угроза безопасности информации, связанная с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении наиболее важных (критичных) информационных систем и баз данных
3.4.	Угроза безопасности информации, связанная с использованием продукции, предназначенной для защиты информации (средств защиты информации), не прошедшей в установленном порядке процедуру оценки соответствия
3.5.	Угроза изменения настроек и режимов работы программного обеспечения (далее – ПО), модификация ПО (удаление, искажение или подмена программных компонентов) ИС ИОГВ ЯНАО или средств защиты информации
3.6.	Угроза нарушения конфиденциальности информации посредством ее утечки в ходе ремонта, модификации и утилизации программно-аппаратных средств
3.7.	Угроза предоставления пользователям прав доступа к защищаемым ресурсам информационных систем сверх объема, необходимого для работы
3.8.	Угроза несанкционированного (умышленного либо случайного) копирования защищаемой информации на неучтенные (в том числе отчуждаемые) носители, а также несанкционированная печать копий документов с защищаемой информацией
3.9.	Угроза несанкционированной модификации (преднамеренной либо случайной), уничтожения, фальсификации информационных ресурсов ИС ИОГВ ЯНАО
3.10.	Угроза подключения к ИС ИОГВ ЯНАО стороннего оборудования (компьютеров, дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи)
3.11.	Угроза использования оборудования, оставленного без присмотра, незаблокированных рабочих станций, использования чужих имен и паролей
3.12.	Угроза использования нетрадиционных каналов (например, стеганографии) для передачи защищаемой информации в сторонние ИС и сети связи
3.13.	Угроза копирования защищаемой информации на неучтенные машинные носители
3.14.	Угроза передачи защищаемой информации по открытым каналам связи за пределы контролируемой зоны
3.15.	Угроза использования для обработки защищаемой информации

1	2
	неучтенных программ
3.16	Угроза нарушения установленного порядка резервного копирования данных
3.17.	Угроза нарушения установленных парольных политик, требований к формированию периодичности и порядку смены паролей
3.18.	Угроза разглашения пользовательских имен и паролей, ключевой информации. Использование для входа в систему чужих идентификаторов и паролей (угроза аутентификации)
3.19.	Угроза нарушения правил хранения информации ограниченного доступа, ключевой, парольной и аутентифицирующей информации
3.20.	Угроза предоставления доступа к защищаемой информации, техническим средствам ИС ИОГВ ЯНАО и средствам защиты информации посторонним лицам
3.21.	Угроза подготовки и проведения атак на средства криптографической защиты информации (далее – СКЗИ) и компоненты среды функционирования СКЗИ на этапе эксплуатации при нахождении в пределах контролируемой зоны
3.22.	Угроза отсутствия информирования и своевременного реагирования на инциденты информационной безопасности
4.	Угрозы НСД, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей (угрозы удаленного доступа)
4.1.	Угрозы анализа сетевого трафика с перехватом передаваемой из ИС и принимаемой в ИС из внешних сетей информации
4.2.	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИС, топологии сети, открытых портов и служб, открытых соединений и др.
4.3.	Угрозы внедрения ложного объекта как в ИС, так и во внешних сетях
4.4.	Угрозы подмены доверенного объекта
4.5.	Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных
4.6.	Угрозы выявления паролей
4.7.	Угрозы типа «Отказ в обслуживании»
4.8.	Угрозы удаленного запуска приложений
4.9.	Угрозы внедрения по сети вредоносных программ
5.	Угрозы внедрения вредоносных программ (программно-математического воздействия)
5.1.	Угрозы внедрения вредоносных программ (программно-математического воздействия) с использованием отчуждаемых носителей информации
5.2.	Угрозы внедрения вредоносных программ (программно-математического воздействия) с использованием сетей связи общего доступа
6.	Угрозы техногенного характера

1	2
6.1.	Угрозы сбоя и (или) выхода из строя технических средств, программных средств и (или) средств защиты информации ИС ИОГВ ЯНАО
6.2.	Угрозы сбоев и аварий на системах обеспечения ИС ИОГВ ЯНАО (электропитание, заземление, теплоснабжение и иные случайные факторы)
7.	Угрозы безопасности информации, размещенные на официальном сайте Федеральной службы по техническому и экспортному контролю (http://bdu.fstec.ru)